

FILED

FEB 19 2016

U.S. COURT OF
FEDERAL CLAIMS

ORIGINAL

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN,

Plaintiff,

V.

UNITED STATES,

Defendant.

1:13-cv-307-SGB

Judge Susan G. Braden

February 18, 2016

PLAINTIFF'S CLAIM CHART

On December 22, 2015, the court convened a telephone status conference.

Pursuant to the status conference, the court grants Plaintiff leave to file an amended complaint by February 15, 2016. The court will convene another telephone status conference on March 1, 2016. Plaintiff will submit a claims chart by March 15, 2016.

Pursuant to the Court's December 22, 2015, Order, ECF No. 65, Plaintiff is hereby submitting a Claims Chart. (Exhibit A)

PLAINTIFF LARRY GOLDEN makes the following allegations in support of its claim for relief.

PARTIES

1. Plaintiff Larry Golden is a citizen of South Carolina and has a principal place of business at 740 Woodruff Road, #1102, Greenville, S.C. 29607.

2. The United States is the Defendant to this action based upon the actions and conduct of its agents, including at least the following agencies: Department of Homeland Security (DHS), Domestic Nuclear Detection Office (DNDO), Department of Defense (DoD),

U.S. Defense Advanced Research Projects Agency (DARPA), National Science Foundation (NSF), Department of Air Force (DOAF), National Institutes of Health (NIH), National Aeronautics and Space Administration (NASA), Department of Energy (DOE), Department of the Army (DOA), U.S. Army Edgewood Chemical Biological Center (ECBC), Army Research Laboratory (ARL), Department of the Navy (DON), U.S. Naval Air Systems Command (NAVAIR), Office of Naval Research's (ONR), U.S. Naval Research Laboratory (NRL), U. S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC), Defense Threat Reduction Agency (DTRA), Environmental Protection Agency (EPA), and Federal Emergency Management Agency (FEMA) (collectively "Unlicensed Manufactures").

3. Plaintiff has submitted a list of Government Agencies and Government Representatives Plaintiff gave notice of Plaintiff's patented claims, patent pending claims, and subject matter disclosed within the patent(s) specifications. (ECF No. 68)

JURISDICTION

4. This is a claim pursuant to 28 U.S.C. §§ 1498(a) and 1491(a) for recovery of Plaintiff's reasonable and entire compensation for the unlicensed use and manufacture, for and by the United States, of inventions described in and covered by United States Patent Numbers: 7,385,497; 7,636,033; 8,106,752; 8,334,761; 8,531,280; RE43,891; RE43,990; 9,096,189; and Published Patent Application No. 2016-0027273 A1

5. The jurisdiction of this Court is based on the provisions of 28 U.S.C. §§ 1498(a) and 1491(a).

FACTUAL BACKGROUND

6. The patents asserted in this Claim Chart (Exhibit A) are U.S. Patent No. 7,385,497 ("497 Patent") (ECF No. 68), U.S. Patent No. 8,106,752 ("752 Patent") (ECF No.

68), U.S. Reissue Patent No. RE43,891 (“891 Patent”) (ECF No. 68), U.S. Reissue Patent No. RE43,990 (“990 Patent”) (ECF No. 68), and U.S. Patent No. 9,096,189 (“189 Patent”) (ECF No. 68)

7. The above listed patents are lawfully issued, valid, and enforceable U. S. Patents.

8. Plaintiff is the sole owner of the entire right, title, and interest in and to the above listed patents.

PRAYER

WHEREFORE, Plaintiff respectfully requests judgment in its favor against the United States granting Plaintiff the following relief:

9. Entry of judgment that the inventions set forth in the '497; '752; '891; '990; and '189 patents have been used and manufactured by and for the United States without license or lawful right within the meaning of 28 U.S.C. § 1498(a);

10. Reasonable and entire compensation for the unlicensed use and manufacture by and for the United States of multi-sensor devices covered by and described in the '497; '752; '891; '990; and '189 patents under 28 U.S.C. § 1498(a), in an amount to be determined at trial;


11. Plaintiff's reasonable fees for expert witnesses and attorneys, plus its costs in accordance with 28 U.S.C. §§ 1498(a) and 1491(a);

12. Pre-judgment and post-judgment interest on Plaintiff's award; and

13. All such other relief that the Court deems just and proper.

14. Leave to add additional alleged infringement products, devices or services and additional patents and patent claims.

Respectfully submitted,

s/ 
Larry Golden
Plaintiff, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 18th day of February, 2016, a true and correct copy of the foregoing CLAIMS CHART § 1498(a) was served upon the following defendant by the methods indicated below:

Kirby W. Lee
Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
(by Certified Mail)

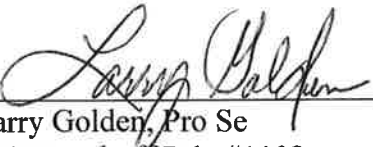
s/ 
Larry Golden, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net

EXHIBIT A:

CLAIMS CHART

CLAIM CHART OUTLINE: LARRY GOLDEN vs. THE UNITED STATES (CASE NUMBER: 13-307 C)

Page 1

"TOUGHBOOK 31" Laptop K-Max Self-flying Helicopter	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
---	---	---

Page 5

K-Max Self-flying Helicopter	Patent #: RE 43,891; Independent Claim 44	Patent #: RE 43,891; Dependent Claims (55, 45, 48, 53, 52)
------------------------------	--	---

Page 8

Apple iPad Tablet Boeing MH-6 Little Bird Helicopter	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
---	---	---

Page 13

Boeing MH-6 Little Bird Helicopter	Patent #: RE 43,891; Independent Claim 23	Patent #: RE 43,891; Dependent Claims (55, 27, 31, 30)
------------------------------------	--	---

Page 18

iControl Inc. "mLOCK"	Patent #: RE 43,990; Independent Claim 125	Patents: 8,106,752; RE 43,990; Dependent Claims (36); (148, 135, 35, 39, 44)
-----------------------	---	--

Page 21

NRL: SIN-VAPOR / Smartphone System	Patent #: 9,096,189; Independent Claim 4	Patent #: RE 43,990; Dependent Claims (118, 122, 124, 108)
---------------------------------------	---	---

Page 26

Smartphone (iPhone) Microscope	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims (118, 17, 92, 25, 12, 124, 99)
--------------------------------	--	--

Page 31

Samsung Galaxy s6 "BioPhone"	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
------------------------------	--	--

Page 35

Samsung Galaxy s6 "Microscope" Smartphone	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims (118, 17, 92, 25, 12, 124, 99)
---	--	--

Page 40

"VOCKET System" / "Nett Warrior" Smartphone System	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims (119, 17, 124, 108)
--	--	---

Page 44

Eureka Aerospace High Powered Electromagnetic System, or HPEMS	Patent #: RE 43,891; Independent Claim 11	Patent #: RE 43,891; Dependent Claims (19, 15, 21)
--	---	--

Page 49

Northrop Grumman X-47B UCAS X-47B Control Display Unit (CDU)	Patent #: RE 43,891; Independent Claim 11	Patent #: RE 43,891; Dependent Claims (19, 27, 15, 21)
--	---	--

Page 56

GammaPix for Android Smartphones	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims (119, 17, 124, 108)
---	---	--

Page 61

Smartphone (iPhone) Biosensor "Cradle"	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims (118, 17, 92, 25, 12, 124, 99)
---	---	---

Page 66

MIT: "NFC" Samsung Galaxy s6 Smartphone Sensor	Patent #: 9,096,189; Independent Claim 3	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20)
---	---	---

Page 70

"Cell-All": Synkera MikroKera Ultra	Patent #: 7,385,497; Independent Claim 1	Patents: 7,385,497; 8,106,752; & RE 43,990; Dependent Claims (2, 4); (34, 37); (119, 29)
--	---	---

Page 74

"Cell-All": Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims (34); (18, 12, 28, 25, 20, 124)
--------------------------------------	---	--

Page 79

"Cell-All": Apple iPhone	Patent #: 9,096,189; Independent Claim 8	Patents: 8,106,752; & RE 43,990; Dependent Claims (34); (118, 17, 92, 25, 124)
---------------------------------	---	---

Page 85

"Biotouch" Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
-------------------------------------	---	---

Page 90

"Biotouch System" / "Nett Warrior" Smartphone System	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims (119, 17, 124, 108)
---	---	--

Page 95

iPhone "Biodelector" Smartphone	Patent #: 9,096,189; Independent Claim 4	Patent #: RE 43,990; Dependent Claims (118, 122, 124, 108)
--	---	---

Page 100

"PathTracker" An iPhone-based Detection Instrument	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims (118, 17, 92, 25, 12, 124, 99)
---	---	---

Page 105

Navy Marine Corps Intranet (NMCID) Network - Apple iPad	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
--	---	---

Page 110

Navy Marine Corps Intranet (NMCID) Network - Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims (34); (18, 12, 28, 25, 20, 124)
---	---	--

Page 115

Navy Marine Corps Intranet (NMCI) Network - Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 3	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20)
--	---	---

Page 120

FLIR: identifiFINDER R300 / Smartphone System	Patent #: 9,096,189; Independent Claim 4	Patent #: RE 43,990; Dependent Claims (118, 122, 124, 108)
--	---	---

Page 127

AOptix Stratus MX Peripheral for the Apple (iPhone) Smartphone	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims (118, 17, 92, 25, 12, 124, 99)
---	---	---

Page 133

MultiRae Pro Wireless Portable Multi Threat Radiation and Chemical Detector	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims (119, 79, 124, 78)
--	---	---

Page 139

PositiveID - Boeing / M-Band Apple (iPhone) Smartphone	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims (118, 17, 92, 25, 12, 124, 99)
---	---	---

Page 145

PositiveID / "Firefly DX" Samsung Galaxy s6 Smartphone	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
---	---	---

Page 150

2"x2" Detection Device (DD) Samsung Galaxy s6 Smartphone	Patent #: 7,385,497; Independent Claim 1	Patents: 7,385,497; 8,106,752; & RE 43,990; Dependent Claims (2, 4); (34, 37); (119, 29)
---	---	---

Page 154

1"x2" Detection Device (DD) Samsung Galaxy s6 Smartphone	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims (34); (18, 12, 28, 25, 20, 124)
---	---	--

Page 159

Nets² SmartShield G300 Radiation Detector Samsung Galaxy s6 Smartphone	Patent #: 7,385,497; Independent Claim 1	Patents: 7,385,497; 8,106,752; & RE 43,990; Dependent Claims (2, 4); (34, 37); (119, 29)
---	---	---

Page 163

Nets² SmartShield G500 Radiation Detector Samsung Galaxy s6 Smartphone	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims (34); (18, 12, 28, 25, 20, 124)
---	---	--

Page 168

"TOUGHBOOK 31" Laptop Passport Systems Inc. Base Control Unit (BCU)	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
--	---	---

Page 173

Oshkosh Defense Autonomous Unmanned Ground Vehicle (UGV) "TerraMax"	Patent #: RE 43,891; Independent Claim 44	Patent #: RE 43,891; Dependent Claims (55, 27)
--	--	---

Page 177

Dream Hammer's "Ballista" Software for Computer, Tablet or Smartphone	Patent #: RE 43,891; Independent Claim 44	Patent #: RE 43,891; Dependent Claims (55, 27)
--	--	---

Page 181

"COINS" Nano-Embedded Sensors for Smartphones	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
--	---	---

Page 186

Variable's "NODE+Oxa" for the Apple (iPhone) Smartphone	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
--	---	---

Page 191

Smartphone-Based Rapid Diagnostic Tests	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims (18, 12, 28, 25, 20, 32, 30)
--	---	---

"TOUGHBOOK 31" Laptop K-Max Self-flying Helicopter	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>The Lockheed Martin K-Max unmanned helicopter is controlled from a Panasonic "TOUGHBOOK 31" Laptop. K-Max has pre-programmed load pick-ups; can fly to pre-programmed and non pre-programmed locations; controller uses beyond-line-of-sight (BLOS) from a video camera mounted in cockpit.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>
<p>CPU: Intel® Core™ i5-3380M vPro™ Processor; 2.9GHz with Turbo Boost up to 3.6GHz; Intel Smart Cache 3MB; Intel® Core™ i5-3340M vPro™ Processor; 2.7GHz with Turbo Boost up to 3.4GHz; Intel Smart Cache 3MB; Intel® Core™ i3-3120M Processor; 2.5GHz; Intel Smart Cache 3MB</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>Hard Disk Lock; Kensington cable lock slot</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

Hard Disk Lock; Kensington cable lock slot	a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Optional integrated 4G LTE multi carrier mobile broadband with satellite GPS; Optional GPS (SiRFstarIII™); Intel® Centrino® Advanced-N 6235 802.11a/b/g/n; Bluetooth® v4.0 + EDR (Class 1);	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Wireless: n Optional integrated 4G LTE multi carrier mobile broadband with satellite GPS; Optional GPS (SiRFstarIII™); Intel® Centrino® Advanced-N 6235 802.11a/b/g/n; Bluetooth® v4.0 + EDR (Class 1); Security; Authentication: LEAP, WPA, 802.1x, EAP-TLS, EAP-FAST, PEAP; Encryption: CKIP, TKIP, 128-bit and 64-bit WEP, Hardware AES; User-selectable antenna pass-through (dual standard, single optional); Slide on/off switch	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.

<p>Security features: Password Security; Supervisor, User, Hard Disk Lock; Kensington cable lock slot; Trusted platform module (TPM) security chip v.1.22; Computrace theft protection agent in BIOS8; Intel® Anti-Theft Technology; Optional fingerprint reader; Optional insertable SmartCard reader</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>Integrated Options: 4G LTE multi carrier mobile broadband with satellite GPS; GPS (SiRFstarIII™); Webcam2; 2nd LAN (10/100)2 or Modem; Insertable SmartCard reader; Fingerprint reader; Media bay 2nd battery¹</p> <p>Security features: Password Security; Supervisor, User, Hard Disk Lock; Kensington cable lock slot; Trusted platform module (TPM) security chip v.1.22; Computrace theft protection agent in BIOS8; Intel® Anti-Theft Technology; Optional fingerprint reader; Optional insertable SmartCard reader</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>Bluetooth® v4.0 + EDR (Class 1)</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Fingerprint reader. Security; Authentication: LEAP, WPA, 802.1x, EAP-TLS, EAP-FAST, PEAP</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>Optional integrated 4G LTE multi carrier mobile broadband with satellite GPS; Intel® Centrino® Advanced-N 6235 802.11a/b/g/n; Bluetooth® v4.0 + EDR (Class 1)</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

"K-Max Self-flying Helicopter"	Patent #: RE 43,891; Independent Claim 44	Patent #: RE 43,891; Dependent Claims
<p>The K-MAX self-flying vehicle can be flown by a human sitting in the cockpit, but it cannot be completely remotely piloted; someone on ground controlling everything the helicopter does. A ground controller can, however, use satellite communication and a laptop to change the mission at any point during flight. Retrofitted Device: Autonomous Aerial Cargo/Utility System (AACUS)</p>	<p>A vehicles' stall-to-stop system or vehicle slowdown system in signal communication with a pre-programmed automated system is adapted, modified, or designed to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:</p>	<p>55. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.</p>
<p>NASA has identified LIDAR as a key technology for enabling autonomous precision safe landing of future robotic and crewed lunar-landing vehicles. Lidar sensors that are mounted on mobile platforms such as airplanes. Components to a LIDAR system: Laser 2-Scanner and optics 3- Photodetector and receiver electronics 4-Position and navigation systems</p>	<p>an electrical system in electrical communication with at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;</p>	<p>45. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
<p>K-max is equipped with Autonomous Aerial Cargo/Utility System (AACUS) technology, which combines advanced algorithms with LIDAR. Lidar uses ultraviolet, visible, or near infrared light to image objects. LIDAR instruments fitted to aircraft and satellites carry out surveying and mapping.</p>	<p>a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>48. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle system designed to perform as a pre-crash system for stopping or slowing a vehicle to prevent a crash.</p>

<p>NASA has identified LIDAR as a key technology for enabling autonomous precision safe landing of future robotic and crewed lunar-landing vehicles. Lidar sensors that are mounted on mobile platforms such as airplanes. Components to a LIDAR system: Laser 2-Scanner and optics 3- Photodetector and receiver electronics 4-Position and navigation systems</p>	<p>a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means</p>	<p>45. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
<p>K-max is equipped with Autonomous Aerial Cargo/Utility System (AACUS) technology, which combines advanced algorithms with LIDAR. Lidar uses ultraviolet, visible, or near infrared light to image objects. LIDAR instruments fitted to aircraft and satellites carry out surveying and mapping. Lockheed tossed in actuators to physically move the controls in response to electronic commands and added mission computers to tell them what to do, and a 3D imaging system to look out for suitable landing spots.</p>	<p>a receiver in computer communication with the computer system and adapted to receive at least one control signal in response to one of the vehicle's operating systems for monitoring the vehicle's condition upon exceeding a pre-programmed vehicle operating system parameter from the pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means such that the speed of the vehicle is initially decreased immediately after activation of the means upon initial receipt of the at least one control signal; and</p>	<p>53. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle system designed to perform as an adjusted cruise control system for stopping or slowing a vehicle to prevent a crash.</p>

<p>Lockheed Martin OPTIMUS technology aboard a K-MAX unmanned helicopter showcased its autonomous capabilities in March 2014 as part of the Office of Naval Research Autonomous Aerial Cargo/Utility System (AACUS). During the demonstration, an active duty Marine interfaced with the mission system's handheld flight control device to complete a resupply mission. The system successfully planned, routed and executed the mission without user input.</p>	<p>wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor.</p>	<p>52. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle system designed to perform as a remote vehicle slowdown system for stopping or slowing a vehicle by remote means.</p>
---	--	---

<p>Apple iPad Tablet Boeing MH-6 Little Bird Helicopter</p>	<p>Patent #: 9,096,189; Independent Claim 1</p>	<p>Patent #: RE 43,990; Dependent Claims</p>
<p>Navy engineers developed a Carbon Monoxide Sensor package that turns any helicopter with a digital flight control system into an autonomous cargo delivery robot. An authorized person is able to land a full-size Aurora Flight Services little bird helicopter by simply touching a map application on a handheld tablet computer, said Chief of Naval Research Rear. Adm. Matthew Klunder. With an iPad the system can autonomously deliver supplies.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>
<p>Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. Apple A4 is based on the ARM processor architecture. The first version released runs at 1 GHz for the iPad and contains an ARM Cortex-A8 CPU core.</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPad to connect to the internet anywhere cell phone works, to check emails.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi).</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>

<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Apple iPad communication device receives signals from the products to be monitored (e.g. Aurora Flight Services Little Bird Helicopter; the Autonomous Aerial Cargo/Utility System--AACUS) and any of the products grouped by similarities of design.</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPad to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Apple's "Touch ID"; a fingerprint identity sensor that makes it easy to get into the iPad device. The biometric "Touch ID" is used with the iPhone 5s or later, iPad Pro, iPad Air 2, or iPad mini 3 or later.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>

<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPad to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
--	--	--

Boeing MH-6 Little Bird Helicopter	Patent #: RE 43,891; Independent Claim 23	Patent #: RE 43,891; Dependent Claims
<p>Navy engineers have developed a Carbon Monoxide Sensor package that can turn any helicopter with a digital flight control system into an autonomous cargo delivery robot. The system is called the autonomous aerial cargo/utility system, or AACUS; a 20-year-old lance corporal was able to land a full-size Aurora Flight Services Little Bird helicopter by simply touching a map application on a handheld tablet computer</p>	<p>A vehicle adapted for receipt of a signal from a pre-programmed automated system to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:</p>	<p>55. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.</p>
<p>We implemented the emergency maneuver trajectories to ensure the safety of the autonomous Unmanned Little Bird Helicopter, equipped with a large field of view range sensors. The dynamic constraints of the helicopter are given. Given these constraints we approximate five hundred trajectories each forming a positive control invariant set.</p>	<p>at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>The Aurora Flight Services Little Bird helicopter's electrical system serves many electrical sub-systems. It is used to safely power avionics, store electrical energy with which to power up the engine, operate actuators, and power internal and external lights, fans, etc. Autonomous control systems for unmanned aerial vehicles eliminate the need for an operator by substituting intelligent control software and electronics.</p>	<p>an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>Emergency maneuver takes the system out of an undesired configuration. (a) Since we run the experiment with a gradient based optimizer. This lies in a local minimum between two walls of the grand canyon (b) The system follows this path since the future point is safe (c) The future point is no longer safe and an emergency maneuver is selected (d) The optimizer is now in a configuration where it can find a safe path again.</p>	<p>a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>The Aurora Flight Services Little Bird helicopter's electrical system serves many electrical sub-systems. It is used to safely power avionics, store electrical energy with which to power up the engine, operate actuators, and power internal and external lights, fans, etc. Autonomous control systems for unmanned aerial vehicles eliminate the need for an operator by substituting intelligent control software and electronics. An electrical receiver is the part in a complete circuit that receives the electrical energy</p>	<p>a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>Emergency maneuver takes the system out of an undesired configuration. (a) Since we run the experiment with a gradient based optimizer. This lies in a local minimum between two walls of the grand canyon (b) The system follows this path since the future point is safe (c) The future point is no longer safe and an emergency maneuver is selected (d) The optimizer is now in a configuration where it can find a safe path again.</p>	<p>a receiver in computer communication with the computer system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>The Aurora Flight Services Little Bird helicopter's electrical system serves many electrical sub-systems. It is used to safely power avionics, store electrical energy with which to power up the engine, operate actuators, and power internal and external lights, fans, etc. Autonomous control systems for unmanned aerial vehicles eliminate the need for an operator by substituting intelligent control software and electronics. An electrical receiver is the part in a complete circuit that receives the electrical energy</p>	<p>wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>The Aurora Flight Services Little Bird helicopter's electrical system serves many electrical sub-systems. It is used to safely power avionics, store electrical energy with which to power up the engine, operate actuators, and power internal and external lights, fans, etc. Autonomous control systems for unmanned aerial vehicles eliminate the need for an operator by substituting intelligent control software and electronics. An electrical receiver is the part in a complete circuit that receives the electrical energy</p>	<p>wherein the receivers, the computer system, and the electrical system are part of at least one pre-programmed operating system of unintended acceleration, pre-crash, reverse acceleration, stabilization, lane departure, cruise control, driverless vehicle, and chemical biological radiological nuclear explosive (CBRNE) detection;</p>	<p>31. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when the vehicle is in forward movement, backward or reverse movement, side movement, cruise control movement, or lane departure movement or when the vehicle moves outside a designated perimeter or zone.</p>

<p>We implemented the emergency maneuver trajectories to ensure the safety of the autonomous Unmanned Little Bird Helicopter, equipped with a large field of view range sensors. The dynamic constraints of the helicopter are given. Given these constraints we approximate five hundred trajectories each forming a positive control invariant set. The emergency maneuver library rescues the helicopter and immediately takes the system out of an undesired configuration.</p>	<p>wherein the control signal to activate the stall-to-stop or vehicle slowdown is not remote from the vehicle and the signal to activate is initiated when at least one of the vehicle's operating systems for monitoring the vehicle's condition exceeds a pre-programmed vehicle operating system parameter.</p>	<p>30. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is an in-vehicle notification warning of: crash, vehicle parking, speeding; driving too fast for conditions; construction zone; school zone; accident ahead; brake failure; acceleration/deceleration failure; acceleration/deceleration cruise control.</p>
---	---	---

iControl Inc. "mLOCK"	Patent #: RE 43'990; Independent Claim 125	Patents: 8,106,752; RE 43,990; Dependent Claims
<p>The DHS "TRUST" system Communication Requirements. iControl Inc. locking seal "M-Lock". M-Lock's critical parameter is anti-tamper, multi-modal wireless connectivity. M-Lock's critical function is physical security, location and alerting; and, is available where wireless connectivity is available. 26. A method for autonomous operation of a locking device based on a status of the locking device as recited in claim 23, wherein the one or more sensors include one or more of a movement sensor, a temperature sensor, a humidity sensor, an infrared sensor, a radioactivity detection sensor, an acoustic sensor, and a chemical detection sensor. (Patent application: mLOCK Device and Associated Methods; US 20100283575 A1)</p>	<p>A multi-sensor detection system for monitoring products and capable of operating with at least one of a designated perimeter sensor, a range sensor, a human sensor, a light sensor, a video sensor, a tampering sensor, a breach sensor, a temperature sensor, or a door sensor for an unauthorized or unscheduled door opening, comprising:</p>	<p>148. The multi sensor detection security systems [of claim 145], further including at least one sensor of system failure, motion, infrared, perimeter, temperature, tampering or breach, for the prevention of terrorist activity and theft.</p>
<p>A user may connect a computing device, such as a handheld computing device or laptop computer, to the data interface 123 to communicate with the LDD 111 or processor 103. A current proximity of the locking device to a wireless communication network to which the computing system can wirelessly communicate.</p>	<p>at least one communication device of a cell phone, a cell phone detector case, a smart phone, a handheld, a PDA, a laptop, or a computer terminal at a monitoring site, and wherein the communication device has a central processing unit (cpu);</p>	<p>135. The multi-sensor detection system [of claim 125] wherein the internal or external remote/electrical lock disabler is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.</p>

<p>A current proximity of the locking device to a wireless communication network to which the computing system can wirelessly communicate, a temperature near the locking device, a humidity near the locking device, a radioactivity level near the locking device, a chemical presence near the locking device, and an external movement near the locking device.</p>	<p>at least one sensor that is a designated perimeter sensor, range sensor, human sensor, light sensor, video sensor, tampering sensor, breach sensor, temperature sensor, or door sensor for unauthorized or unscheduled door opening, interconnected to the at least one communication device for communication therebetween;</p>	<p>35. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device is designed to unlock or enable the lock of the product thus allowing access to the product by authorized, trained, and equipped individuals.</p>
<p>Upon arrival at the airport, a TSA agent looks at the mLOCK 100 user interface display 144 to see if an alarm was generated in route. If so, the mLOCK 100 is removed and the truck is inspected. If not, the mLOCK 100 is removed and returned to the freight forwarder for use in future shipments. [W]herein some of the one or more sensors proximate to the locking device are physically attached to the locking device and communicate data with the computing system through wired connections.</p>	<p>wherein the at least one interchangeable sensor is interconnected to an internal or external remote/electrical lock disabler;</p>	<p>36. The automatic/mechanical lock disabler system [of claim 35] wherein the automatic/mechanical lock disabler [of claim 35] includes a plurality of interchangeable and integrable sensors for detecting the chemical, biological, radiological, nuclear, explosive and contraband agents and compounds to include sensors for detecting humans, motion, temperature, shock and tampering which is capable of being disposed within the detector case. Patent 8,106,752</p>
<p>3. A locking device as recited in claim 2, further comprising: a solar film electrically connected to the power source and defined to electrically re-charge the power source. 4. A locking device as recited in claim 1, wherein the radio is an international frequency radio, and wherein the location determination device is a global positioning system receiver device.</p>	<p>at least one of an Internet connection, a GPS connection, or a power connection disposed within the internal or external remote/electrical lock disabler;</p>	<p>39. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device has a power connection which is interconnected to the central processing unit (cpu) and includes a power source of battery, electrical or solar.</p>

<p>The mLOCK 100 is an electronic lock that secures an asset, such as cargo within a shipping container, by controlling the ability to operate a locking mechanism of the mLOCK 100 based on proximity to secure networks, geographic locations, or via user commands through a radio link. Based on the automatically determined real-time status of the locking device, operating the computing system to automatically control a locking mechanism of the locking device to either lock or unlock the locking device. The locking mechanism of the mLOCK 100 is secured through a mechanical mechanism that inhibits opening a shackle of the mLOCK 100 unless an electro-mechanical lock actuator 146 enables such operation of the mLOCK 100.</p>	<p>wherein the internal or external remote/electrical lock disabler communicates with the communication device and the internal or external remote/electrical lock disabler is mounted, embedded, affixed, or attached to a product for receiving transmission from the communication device to lock or disable a lock on the product and to prevent access to the product by unauthorized, untrained, and unequipped individuals, wherein the internal or external automatic/mechanical lock disabler detection device engages the lock on the product; and</p>	<p>35. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device is designed to unlock or enable the lock of the product thus allowing access to the product by authorized, trained, and equipped individuals.</p>
<p>17. A method for autonomous operation of a locking device based on a status of the locking device, comprising: operating a computing system onboard the locking device to automatically determine a real-time status of the locking device. The data signal may be a push button signal, an intrusion alarm signal, a chemical/biological agent detection signal, a temperature signal, a humidity signal, or essentially any other type of signal that may be generated by a sensing device.</p>	<p>whereupon detection causes a signal to be sent to the at least one communication device followed by communicating with the internal or external remote/electrical lock disabler.</p>	<p>44. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to a cell phone, smart phone, PDA or handheld device.</p>

NRL: SIN-VAPOR / Smartphone System	Patent #: 9,096,189; Independent Claim 4	Patent #: RE 43,990; Dependent Claims
<p>Developed by the U.S. Naval Research Laboratory (NRL) in Washington, D.C., the silicon nanowires in a vertical array with a porous electrode (SIN-VAPOR) sensor: In addition to detecting chemical weapons or explosives, the sensor can be used for identifying biological agents Dr. Christopher Field, the lead NRL scientist on the SIN-VAPOR research team is working with the NRL's biological research group to apply the sensor in this area.</p>	<p>A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>The SIN-VAPOR ideally allows a sensor to separately identify chemical compounds and gasses in different mixtures, such as TNT, ammonium and carbon dioxide. In addition to detecting chemical weapons or explosives, the sensor can be used for identifying biological agents Dr. Christopher Field, the lead NRL scientist on the SIN-VAPOR research team is working with the NRL's biological research group to apply the sensor in this area.</p>	<p>comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>

<p>By using easily produced super-small components, the devices potentially can be installed in a variety of devices, such as smartphones, robots or commercial appliances. Another goal is to install a sensor on a Google Nexus 7 tablet computer and conduct some wireless sensor networking. Fields explain, adding that the final form factor for the complete sensor will be smaller and likely to be integrated in other handheld or wearable devices.</p>	<p>comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>Touch ID is a fingerprint recognition feature, designed and released by Apple Inc., and is currently available on the iPhone 5S, iPhone 6, iPhone 6 Plus, iPhone 6s, iPhone 6s Plus, iPad Air 2, iPad Pro, and the iPad Mini 3 and iPad Mini 4. Android Marshmallow is here. There are battery life improvements, greater app permission controls, and standardized support for fingerprint scanners. Right now the Nexus 5, Nexus 6, Nexus 7 (2013), Nexus 9, Nexus Player and the whole range of Android One smartphones are getting the latest Android update.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>122. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>

<p>One way to obtain ubiquitous sensing would be to install the SiN-VAPOR arrays in mobile devices. A smartphone already has microphones and cameras—its ears and eyes. Installing this capability into a mobile device effectively turns it into a multipurpose sensor.</p> <p>“Is it TNT from a land mine, an IED [improvised explosive device] or is it TNT from the packaging of bullets? You want to be able to distinguish from these different things,” Field states. The sensor ideally allows a sensor to separately identify chemical compounds and gasses in different mixtures, such as TNT, ammonium and carbon dioxide, while factoring in environmental issues such as humidity. There is a great deal of literature for using silicon-based structures as biosensors. Using the sensors in medical applications, exist as well. The devices potentially can be installed in a variety of devices, such as smartphones. Goal is to install a sensor on a Google Nexus 7 tablet computer.</p>	<p>wherein the built-in embedded multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories; and</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

<p>Dr. Chris Field explains in a video for Tech Briefs TV, the SiN-VAPOR sensor is about the size of a quarter and could be attached to mobile devices, like smartphones, and carried onto the battlefield. "If every soldier has the sensors, and are on a communication network such as a cell phone, they can all talk to each other," Field says. "All the sensors can communicate with each other and you can begin to map the area from a chemical [perspective]." This capability has widespread potential for both military and civilian applications, including biochemical and biomedical applications and sensing of chemical and biological agents, explosives, and toxic industrial chemicals.</p>	<p>wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-long or short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for communication therebetween;</p>	<p>108. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).</p>
---	--	---

<p>The sensors based on SiN-VAPOR is embedded on a silicon chip that is able to integrate in other handheld devices such as wrist watches, smartphones, motion detectors, unattended ground sensors or wearable communications systems. Such devices could be integrated into the warfighters' and first responders' gear, such sensors could be networked into a persistent, distributed sensor network that could monitor the operating area, airport or protected facilities at all time. Fields explain, "the sensor will be integrated in other handheld or wearable devices". According to Field, the SiN-VAPOR technology could help soldiers, first responders, firefighters, and medical professionals. Improving situational awareness by monitoring the environment, reporting the concentration of toxic fumes or chemical traces that could indicate the presence of explosives, chemical warfare agents, toxic fumes etc.</p>	<p>wherein the built-in embedded multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

Smartphone (iPhone) Microscope	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims
<p>“Smartphone Microscope”. Aydogan Ozcan, a professor at UCLA and his team have created a portable smartphone attachment that can be used to perform sophisticated field testing to detect viruses and bacteria. Optical methods for imaging single biomolecules allow for exploration of their individual behavior and properties at nanoscale, significantly advance our knowledge of molecular biology and biophysics. Funding support for the Ozcan Research Group comes from the Army Research Office, the National Science Foundation, the National Institutes of Health, and the Office of Naval Research. Commercialize through Holomic LLC</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>Optical methods for imaging single biomolecules allow for exploration of their individual behavior and properties at nanoscale, which not only significantly advance our knowledge of molecular biology and biophysics but also provide various diagnostics opportunities for biomedical applications.</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>

<p>Weighing 46 grams — approximately as much as a large egg — the microscope is a self-contained imaging device. The only external attachments necessary are a USB connection to a smart-phone, PDA or computer, which supplies the microscope with power and allows images to be uploaded for conversion into results and then sent to a hospital.</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PCs, and cell phones for the receipt and transmission of signals therebetween.</p>
<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. Apple uses A-GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast initial connection along with improving GPS accuracy.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>The microscope can operate in a transmission mode. Although the sensor captures raw data, a computer is required to reconstruct the images. Workers in the field could use their laptops to process the information or send it over the Internet or mobile phone networks (e.g. cell phone towers) to a remote server. Mobile phones could also have sufficient processing power to do the analysis on the spot. "We are replacing an expensive and bulky, heavy component with computer codes," says Aydogan Ozcan,</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>A software interface running on the smartphone scans the DNA and sends the data to a remote server in the team's laboratory. The servers use the data to measure the length of the DNA strands, and return the results in less than 10 seconds, assuming users have access to an internet connection.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>Cellular carriers have precise GPS measurements of locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range and trilateration to find an area that overlaps among them. Apple uses A-GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast connection along with improving GPS accuracy.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>Translation of these and other existing imaging techniques to field-portable, cost-effective and high-throughput instruments would open up a myriad of new applications in, e.g., point-of-care (POC) medicine, global health and diagnostics fields, among others, and would also positively impact research and educational efforts in developing countries and resource-limited institutions, helping the democratization of advanced scientific instruments and measurement tools. For this broad aim, mobile phones and other consumer electronics devices, including, e.g., tablet PCs and wearable computers, have been emerging as powerful platforms to create cost-effective, portable and readily accessible alternatives to some of the advanced biomedical imaging and measurement tools.</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

<p>A software interface running on the smartphone scans the DNA and sends the data to a remote server in the team's laboratory. The servers use the data to measure the length of the DNA strands, and return the results in less than 10 seconds, assuming users have access to an internet connection.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>iPhone and iPad Touch ID is a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>99. The multi-sensor detection system [of claim 81], wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.</p>
<p>A software interface running on the smartphone scans the DNA and sends the data to a remote server in the team's laboratory. The servers use the data to measure the length of the DNA strands, and return the results in less than 10 seconds, assuming users have access to an internet connection.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

Samsung Galaxy s6 "BioPhone"	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>A Samsung Galaxy s6 "BioPhone" smartphone can measure your heart and breathing rates, even if you're not directly touching it. Researchers at MIT are working on a project called BioPhone that derives biological signals from your smartphone's accelerometer, which they say can capture the small movements of your body that result from the beating of your heart and rising and falling of your chest. This information is useful to base medical diagnoses in real-life conditions and to help track chronic health conditions and effects of therapeutic interventions. Research is based upon work supported by the National Science Foundation (NSF CCF-1029585), Samsung, and the MIT Media Lab Consortium.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>
<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The "Biophone" detection device is the same as the cell phone detection device.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone. The "Biophone" detection device is the same as the cell phone detection device.</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>

<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts.</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>A 122 page report focuses on the evolution of the seven wireless interfaces now found in the high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging. Smartphones today include receivers for GPS (US), GLONASS (Russia), and Beidou COMPASS (China). New regional satellite navigation systems from Japan (QZSS) and India (IRNSS) are being introduced over the coming several years. The Bluetooth Low Energy / Smart standard is migrating to the new v4.2 revision. This new personal area wireless networking standard revision enables some compelling use cases that leading smartphone OEMs are likely to rapidly adopt and deploy. Bluetooth Smart potentially has a role to play in wireless battery charging as a control and status side-channel mechanism, synergistically linking these two wireless subsystems.</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>One major feature that Samsung added to its Galaxy line of smartphones was the heart rate monitor. The health-focused technology heart rate sensor is cleverly positioned on the back of the phone and embedded into the same opening as the LED flash. Samsung only allows you to register 4 fingerprints to set-up the fingerprint scanner; a security feature for easy log-in and lock-out.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

Samsung Galaxy s6 "Microscope" Smartphone	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims
<p>The U.S. Army Edgewood Chemical Biological Center (ECBC) is developing cellphone-based wide-field fluorescent imaging of microbeads for pathogen detection. Scientists at ECBC worked with a team at the University of California, Los Angeles (UCLA), to adapt its prototype of a plastic, clip-on "microscope" to fit a Samsung Galaxy Android phone, commonly used by the Army. This device clips directly over the camera of the Smartphone and operates just like a microscope. The UCLA team is developing the hardware and the software for the device, with ECBC's team providing the diagnostic and detection assays that it will utilize. The team is focused on biological diagnostic tests. ECBC has also partnered with Holomic, LLC, a small business in California.</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>The team is focused on biological diagnostic tests, with a current focus on testing blood and urine for Salmonella typhimurium, a causative agent for food poisoning. In the near future, the team plans to add testing for four additional pathogens.</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>

<p>This device clips directly over the camera of the Smartphone and operates just like a microscope. The user collects a sample, slides it into the device, and snaps a picture using the camera in the cell phone</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>
<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. The Galaxy's GPS satellite-based system can communicate location to applications on the device, such as Google Maps™, for navigation; the ability to tag the location from which the sample was taken, allow for further surveillance and monitoring of that area.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
<p>The U.S. Army Edgewood Chemical Biological Center (ECBC) is developing technology to collect a sample, analyze the results, geotag the location of the sample on Google Maps, and send the results to a laboratory for further review—all from the same Smartphone.</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The results from the device can be stored in the phone and later added to a biosurveillance cloud database, allowing for an electronic archive of data that is available to anyone with access to the cloud.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. The Galaxy's GPS satellite-based system can communicate location to applications on the device, such as Google Maps™, for navigation; the ability to tag the location from which the sample was taken, allow for further surveillance and monitoring of that area.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>The anticipated end-user for the technology is both military and civilian. "This is ideal for the soldier out in the field, in a remote area without a cell tower nearby. He or she can still capture the data and store it until it can be sent back to the command post," said Buckley. "It can also be valuable for clinics or hospitals in underdeveloped areas which may not have sophisticated testing equipment. They are more likely to be able to afford a device like this, which combines the ease and reliability of testing with the ability to communicate the results to a larger facility or organization." "The coolest thing about this technology is that it's taking a common test that's done often in a laboratory and applying what we do here: reduce the size, reduce the cost, and reduce the weight. All with a package that is already being used by civilians and soldiers everywhere," said Buckley.</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The results from the device can be stored in the phone and later added to a biosurveillance cloud database, allowing for an electronic archive of data that is available to anyone with access to the cloud.	wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).
One major feature that Samsung added to its Galaxy line of smartphones was the heart rate monitor. The health-focused technology heart rate sensor is cleverly positioned on the back of the phone and embedded into the same opening as the LED flash. Samsung only allows you to register 4 fingerprints to set-up the fingerprint scanner; a security feature for easy log-in and lock-out.	wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;	99. The multi-sensor detection system [of claim 81], wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.
Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The results from the device can be stored in the phone and later added to a biosurveillance cloud database, allowing for an electronic archive of data that is available to anyone with access to the cloud.	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).

"VOCKET System" / "Nett Warrior" Smartphone System	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims
<p>The Army's Edgewood Chemical Biological Center (ECBC) researchers are refining for Army use a commercial technology that will allow soldiers to accurately and rapidly detect an array of chemical and biological hazards - from mustard agent to anthrax. The VOCKET system is a small electronic device developed at ECBC and even manufactured there, for now, on the center's 3D printers. The device reads the result of chemical detection paper and transmit the results into the Army's network via the soldier-worn "Nett Warrior" smartphone system.</p>	<p>A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>
<p>The VOCKET system is a small electronic device developed at ECBC. The device reads the result of chemical detection paper and transmit the results into the Army's network via the soldier-worn "Nett Warrior" smartphone system. The Net Warrior system is a Samsung Galaxy Note II smartphone worn in a chest-mounted pouch and connected to networked radio such as a Harris Falcon III AN/PRC-152A wideband networking handheld radio or the older General Dynamics AN/PRC-154A Rifleman Radio. The device accurately detect an array of chemical and biological hazards.</p>	<p>a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>The VOCKit system is a small electronic device developed at the Army's Edgewood Chemical Biological Center (ECBC), and even manufactured there, for now, on the center's 3D printers. The device reads the result of chemical detection paper and can then transmit the results into the Army's network via the soldier-worn "Nett Warrior" smartphone system.</p>	<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>
<p>The colorimetric detection assays they are using are placed inside a small plastic hockey puck-shaped cartridge that has a removable plug on one side. Researchers can open that plug and put a drop of a test substance inside so as to expose the assay to a chemical or biohazard.</p> <p><i>Plaintiff Patent 9,096,189, Col. 14; Lines 29-36. "Product grouping 3 (detector case; modified and adapted) include, but are not limited to... detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to..."</i></p>	<p>wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>ECBC already has a device called the SmartCAR, short for "smart color-metric assay reader." That hand-held device was developed by ECBC engineer Colin Graham. The SmartCAR does not read the same color-metric assays that Miklos and Dixon are working on. The SmartCAR, in conjunction with the Nett Warrior device, can run the evaluation, capture the results, and transmit the results, along with latitude, longitude and time to a central location on an Army network so that it can be used by commanders,</p> <p>Emanuel said.</p>	<p>wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
<p>The system is a colorimetric detection assay, a swatch of paper about the size of a postage stamp that is printed with several dozen indicator chemicals arranged in a grid of small dots. Each dot is made from a differently-colored indicator chemical that will have a unique color change in response to any compound it comes in contact with: from chemical threats, to biological threats</p>	<p>a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>The VOCKit system is a small electronic device developed at the Army's Edgewood Chemical Biological Center (ECBC). The device reads the result of chemical detection paper and transmit the results into the Army's network via the soldier-worn "Nett Warrior" smartphone system. The Nett Warrior system is a Samsung Galaxy Note II smartphone worn in a chest-mounted pouch and connected to networked radio such as a Harris Falcon III AN/PRC-152A wideband networking handheld radio or the older General Dynamics AN/PRC-154A Rifleman Radio.</p>	<p>wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.</p>	<p>108. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).</p>
--	---	---

Eureka Aerospace High Powered Electromagnetic System, or HPEMS	Patent #: RE 43,891; Independent Claim 11	Patent #: RE 43,891; Dependent Claims
<p>The U.S. Air Force request for an "air-delivered capability to disable moving ground vehicles while minimizing harm to occupants." Presumably the Air Force wants to look beyond helicopter-mounted snipers, and so Eureka Aerospace's device could potentially fit the bill. The U.S. Marines have lined up as possible customers. The idea is that an electromagnetic pulse (from a remote location) would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. Boeings; as partner provided funds for research.</p>	<p>A vehicle adapted for receipt of a signal from a remote location to control the vehicle's stall-to-stop means or vehicle slowdown means, comprising:</p>	<p>19. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means both have the ability to slowdown or stall the vehicle naturally and without any action on the brakes, door locks, or steering wheel, and both have the ability to slowdown or stall the vehicle through unnatural means where there may be action on the brakes, door locks, and steering for navigation to a safe stop.</p>
<p>The High Powered Electromagnetic System, or HPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse (from a remote location) would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;</p>	<p>19. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means both have the ability to slowdown or stall the vehicle naturally and without any action on the brakes, door locks, or steering wheel, and both have the ability to slowdown or stall the vehicle through unnatural means where there may be action on the brakes, door locks, and steering for navigation to a safe stop.</p>

<p>The High Powered Electromagnetic System, or HPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
<p>The High Powered Electromagnetic System, or HPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>

<p>The High Powered Electromagnetic System, or HPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
<p>The High Powered Electromagnetic System, or HPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>

<p>The High Powered Electromagnetic System, or HPPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
<p>"In an attempt to put an end to dangerous, high-speed police chases, scientists at Eureka Aerospace have developed an electromagnetic pulse gun called the High Power Electromagnetic System, or HPPEMS</p>	<p>wherein the at least one control signal is sent due to unauthorized use of the vehicle, and wherein an originating first signal that eventually causes the at least one control signal to be sent is generated upon initial verification of the unauthorized use of the vehicle;</p>	<p>21. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the products by unauthorized, untrained, and unequipped individuals.</p>

<p>The High Powered Electromagnetic System, or HPEMS develops a high-intensity directed pulse of electricity designed to disable a car's microprocessor system, shutting down all of its systems. The idea is that an electromagnetic pulse would be used to disable a car's microprocessors, chips, and whatever other electronics are keeping it running. The disabling power only works for more modern cars that rely upon microprocessors and various electronics for their engine, as opposed to pre-1970s cars.</p>	<p>at least one mobile, portable, or fixed device capable of sending the at least one control signal from the remote location that is of electromagnetic pulse, electrostatic discharge, microwave beam or radio frequency, to disable the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and horsepower of the motor.</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
--	---	---

Northrop Grumman X-47B UCAS X-47B Control Display Unit (CDU)	Patent #: RE 43,891; Independent Claim 11	Patent #: RE 43,891; Dependent Claims
<p>The U.S. Navy's UCAS-D program is designed to demonstrate the ability of a fighter-sized unmanned aircraft to land on and be launched from the flight deck of a Navy aircraft carrier underway at sea.</p> <p>Northrop Grumman Corporation (NYSE: NOC), a leader in unmanned systems, serves as the Navy's prime contractor for the UCAS-D program, which is managed by U.S. Naval Air Systems Command (NAVAIR). Under contract awarded in Aug. 2007, Northrop Grumman designed the X-47B. From a remote place the X-47B Control Display Unit controls the aircraft's stall, stop, and slow-down means.</p>	<p>A vehicle adapted for receipt of a signal from a remote location to control the vehicle's stall-to-stop means or vehicle slowdown means, comprising:</p>	<p>19. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means both have the ability to slowdown or stall the vehicle naturally and without any action on the brakes, door locks, or steering wheel, and both have the ability to slowdown or stall the vehicle through unnatural means where there may be action on the brakes, door locks, and steering for navigation to a safe stop.</p>
<p>When the Unmanned X-47B aircraft gets on board an aircraft carrier, it's going to be controlled by a "mouse click," Pamijans says. The click of a mouse will turn on the engines. Another will get it to taxi. Keep clicking, and the plane will "take off and come home." No joysticks and no pilot controlling it from a metal box somewhere. Just push-button operations and 3.4 million lines of software code and functionality to control the X-47B.</p>	<p>at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;</p>	<p>19. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means both have the ability to slowdown or stall the vehicle naturally and without any action on the brakes, door locks, or steering wheel, and both have the ability to slowdown or stall the vehicle through unnatural means where there may be action on the brakes, door locks, and steering for navigation to a safe stop.</p>

<p>The X-47B Smart, Autonomous Air System, is a computer-controlled unmanned aircraft system that takes off, flies a preprogrammed mission, and then returns to base in response to mouse clicks from its mission operator. The mission operator monitors the X-47B air vehicle's operation, but does not actively "fly" it via remote control as is the case for other unmanned systems currently in operation.</p>	<p>an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>The X-47B is fully autonomous in flight, relying on computer programs to tell it where it needs to go unless a mission operator needs to step in. That differs from other drones used by the military, which are more often piloted from remote locations.</p>	<p>a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>Nov. 2012: Is the completion date of the shore-based testing of a wireless, handheld X-47B Control Display Unit (used for precision deck handling of X-47B). Northrop Grumman test pilots, Dave Lorenz, and Bruce McFadden, launched the new X-47B off the nuclear aircraft carrier USS George H. W. Bush off the coast of Virginia. They issued orders to the autonomous drone using their forearm-mounted Control Display Units. The Control Display Unit (CDU), is used to control the X-47B's engine thrust to roll the aircraft forward, brake and stop, and use its nose wheel steering to execute the tight, precision turns required to maneuver.</p>	<p>a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
--	---	---

<p>Nov. 2012: Is the completion date of the shore-based testing of a wireless, handheld X-47B Control Display Unit (used for precision deck handling of X-47B). Northrop Grumman test pilots, Dave Lorenz, and Bruce McFadden, launched the new X-47B off the nuclear aircraft carrier USS George H. W. Bush off the coast of Virginia. They issued orders to the autonomous drone using their forearm-mounted Control Display Units. The Control Display Unit (CDU), is used to control the X-47B's engine thrust to roll the aircraft forward, brake and stop, and use its nose wheel steering to execute the tight, precision turns required to maneuver.</p>	<p>a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
--	---	---

<p>Nov. 2012: Is the completion date of the shore-based testing of a wireless, handheld X-47B Control Display Unit (used for precision deck handling of X-47B). Northrop Grumman test pilots, Dave Lorenz, and Bruce McFadden, launched the new X-47B off the nuclear aircraft carrier USS George H.W. Bush off the coast of Virginia. They issued orders to the autonomous drone using their forearm-mounted Control Display Units. The Control Display Unit (CDU), is used to control the X-47B's engine thrust to roll the aircraft forward, brake and stop, and use its nose wheel steering to execute the tight, precision turns required to maneuver.</p>	<p>wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
---	--	---

<p>Milstar II satellites will benefit from a Northrop Grumman-developed digital processing subsystem that delivers data 640 times faster than Milstar I payloads. The digital processing subsystem, combined with the RF subsystem built by Boeing Satellite Systems, constitutes the medium data rate (MDR) payload electronics package. The MDR payload is tailored to meet the needs of third world threats and regional conflicts. Flexible onboard processing instantly reconfigures networks to suit evolving command and control requirements. The use of EHF frequencies and highly directional nulling antennas reduce the probability of jamming and intercept. Lightweight portable terminals on land, sea, and in the air can be easily moved during tactical operations.</p>	<p>wherein the at least one control signal is sent due to unauthorized use of the vehicle, and wherein an originating first signal that eventually causes the at least one control signal to be sent is generated upon initial verification of the unauthorized use of the vehicle;</p>	<p>21. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the products by unauthorized, untrained, and unequipped individuals.</p>
---	---	---

<p>The Control Display Unit (CDU), is used to control the X-47B's engine thrust to roll the aircraft forward, brake and stop. Taxi controllers will have display units mounted on their arms that send radio frequencies to direct the plane across the decks.</p>	<p>at least one mobile, portable, or fixed device capable of sending the at least one control signal from the remote location that is of electromagnet pulse, electrostatic discharge, microwave beam or radio frequency, to disable the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and horsepower of the motor.</p>	<p>15. The stall-to-stop disabling and slowdown system [of claim 11] wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.</p>
--	---	---

GammaPix for Android Smartphones	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims
<p>GammaPix for Android Smartphones (e.g. Samsung Galaxy s6) scans for radiation using a smartphone camera sensor. Scanning for radiation and radioactive explosives the camera looks for a particular 'signature' left behind by gamma rays. It measures the rate at which rays hit the lens to determine radiation levels. App detects radiation in planes, hospitals, contaminated items and more. It was created by Connecticut-based developers Image Insight under a \$679,000 contract with the U.S. Defense Advanced Research Projects Agency (DARPA).</p>	<p>A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>
<p>Gamma radiation, also known as gamma rays, refers to electromagnetic radiation of an extremely high frequency and therefore consists of high-energy photons. Gamma rays are ionizing radiation, and are thus biologically hazardous. Gamma resonance absorption (GRA), which relies on the preferential absorption of particular gamma rays to detect explosives. The GRA system has several features that give it a probability of detection superior to most explosives-detection systems now under development.</p>	<p>a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>GammaPix uses scanning technology that analyses videos and photos taken using a smartphone's camera. The smartphone camera looks for a particular 'signature' left behind by gamma rays, similar to how a Geiger counter or other radiation scanner works. It measures the rate at which these rays hit the camera's sensor to determine radiation levels and will warn users if they are being exposed to harmful rays.</p>	<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>
<p>The GammaPix app measures the rate at which gamma rays hit the smartphone camera's sensor during a scan, to determine radiation levels. A full scan takes around five minutes, pictured left, but will warn a user immediately if a dangerous amount is detected.</p>	<p>wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>In military and federal tests it has been used to detect hazards from simulated terrorist attacks, dirty bombs, or hidden radioactive materials. GammalPix can additionally be used to detect 'radioactivity in everyday life' such as exposure on airplanes, from medical patients or from contaminated products.</p>	<p>wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	--

<p>Gamma-ray sensitivity of CCD and CMOS chips in the cameras' digital image sensors, the image sensor produces bright pixels. The specific color that a pixel describes is some blend of three components of the color spectrum - RGB. Up to three bytes of data are allocated for specifying a pixel's color, one byte for each major color component. A true color or 24-bit color system uses all three bytes. However, many color display systems use only one byte (limiting the display to 256 different colors). Highpass-filters every individual pixel and all three color channel; calculates the average; and, standard distribution of the tremendous amount of 1 byte samples. If the light detector inside the camera would react even weakly with the gamma (and maybe beta) radiation from the minerals, pixels should light up here and there, pushing the distribution wider.</p>	<p>a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>
--	---	---

<p>Image Insight said: 'The technology is sensitive enough to detect, within seconds, dangerously high levels of radiation.' It added, the software also collects and saves radiation records, from minutes to hours, to detect weaker radioactivity sources or normal background radioactivity. The scans are then sent to a central command post through a software called GeoSuite. GeoSuite is currently used to share information with the authorities following a natural disaster.</p>	<p>wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.</p>	<p>108. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).</p>
---	---	---

Smartphone (iPhone) Biosensor "Cradle"	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims
<p>University of Illinois researchers developed a cradle and app for the iPhone to make a handheld biosensor that uses the phone's own camera and processing power to detect any kind of biological molecules or cells. At the heart of the iPhone biosensor is a photonic crystal. When anything biological attaches to the photonic crystal - such as protein, cells, pathogens or DNA - the reflected color will shift. The group received a grant from the National Science Foundation to expand the range of biological experiments that can be performed with the iPhone.</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>A cradle and app for the iPhone to make a handheld biosensor that uses the phone's own camera and processing power to detect any kind of biological molecules or cells. At the heart of the iPhone biosensor is a photonic crystal. When anything biological attaches to the photonic crystal - such as protein, cells, pathogens or DNA - the reflected color will shift.</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>Cradle turns smartphone into handheld biosensor: Smartphone cradle and app may detect bacteria, allergens.</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PCs, and cell phones for the receipt and transmission of signals therebetween.</p>

<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. Apple uses A-GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast initial connection along with improving GPS accuracy.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
<p>Using SOS one-touch smartphone application, the iPhone data is relayed to the control center to include full profile of an exact, GPS based location; Digital Transmission of Distress. The control center will react to any emergency, providing two-way communication enabling real time tracking and alerting.</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>A software interface (app) running on the smartphone scans the pathogens, biomarkers or DNA and sends the data to a remote server at the control center. The servers use the data to measure the results of the scans, and return the results in a short period of time, assuming users have access to an internet connection.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

<p>Cellular carriers have precise GPS measurements of locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range and trilateration to find an area that overlaps among them. Apple uses AGPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast connection along with improving GPS accuracy.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
---	---	--

<p>Translation of these and other existing imaging techniques to field-portable, cost-effective and high-throughput instruments would open up a myriad of new applications in, e.g., point-of-care (POC) medicine, global health and diagnostics fields, among others, and would also positively impact research and educational efforts in developing countries and resource-limited institutions, helping the democratization of advanced scientific instruments and measurement tools. For this broad aim, mobile phones and other consumer electronics devices, including, e.g., tablet PCs and wearable computers, have been emerging as powerful platforms to create cost-effective, portable and readily accessible alternatives to some of the advanced biomedical imaging and measurement tools.</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat, grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

<p>A software interface (app) running on the smartphone scans the pathogens, biomarkers or DNA and sends the data to a remote server at the control center. The servers use the data to measure the results of the scans, and return the results in a short period of time, assuming users have access to an internet connection.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>iPhone and iPad Touch ID is a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>99. The multi-sensor detection system [of claim 81], wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.</p>
<p>A software interface (app) running on the smartphone scans the pathogens, biomarkers or DNA and sends the data to a remote server at the control center. The servers use the data to measure the results of the scans, and return the results in a short period of time, assuming users have access to an internet connection.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

MIT: "NFC" Samsung Galaxy s6 Smartphone Sensor	Patent #: 9,096,189; Independent Claim 3	Patent #: RE 43,990; Dependent Claims
<p>The MIT "NFC" Smartphone sensors are made from modified near-field communication (NFC) tags. These tags, which receive the little power they need from the Samsung Galaxy s6 smartphone reading them, function as wirelessly addressable barcodes. The modified tags are referred to as CARDS: chemically actuated resonant devices. When a smartphone pings the CARD, the CARD responds only if it can receive sufficient power at the smartphone transmitted radio frequencies (RF). MIT's research was funded by the U.S. Army Research Laboratory and the U.S. Army Research Office.</p>	<p>Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>
<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and any of a plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The CARD (chemically actuated resonant device) is the multi-sensor detection device.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone. The CARD (chemically actuated resonant device) is the multi-sensor detection device.</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality of product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>Once an individual phone gathers data, the information could be uploaded to wireless networks and combined with sensor data from other phones, allowing coverage of very large areas. The researchers are also seeking to integrate Bluetooth technology to expand its range beyond 5 cm (2 in). Samsung Galaxy s6 WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency (RF) connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone.</p>	<p>whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>Once an individual phone gathers data, the information could be uploaded to wireless networks and combined with sensor data from other phones, allowing coverage of very large areas. The researchers are also seeking to integrate Bluetooth technology to expand its range beyond 5 cm (2 in). Samsung Galaxy S6 WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency (RF) connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>The MIT "NFC" Smartphone sensors are made from modified near-field communication (NFC) tags. These tags, which receive the little power they need from the Samsung Galaxy s6 smartphone reading them, function as wirelessly addressable barcodes. The modified tags are referred to as CARDS: chemically actuated resonant devices. When a smartphone pings the CARD, the CARD responds only if it can receive sufficient power at the smartphone transmitted radio frequencies (RF). NFC tags can be read by any smartphone that has near-field communication capability, which is included in many newer smartphone models. The Samsung Galaxy s6 smartphones can send out short pulses of magnetic fields at radio frequency (13.56 megahertz), inducing an electric current in the circuit on the tag, which relays information to the phone.</p>	<p>at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency (RF) connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
---	--	---

“Cell-All”: Synkera MikroKera Ultra	Patent #: 7,385,497; Independent Claim 1	Patents: 7,385,497; 8,106,752; & RE 43,990; Dependent Claims
<p>Synkera presented the MikroKera Ultra Module at the Department of Homeland Security S&T “Cell-All” demonstration in Los Angeles on September 28, 2011. Synkera offers a general purpose digital module for evaluation and use of MikroKera Ultra chemical sensors. Synkera Technologies has been funded by DHS to develop sensors that are suitable for integration into cell phones and other ubiquitous electronic devices carried by first responders and the public at large. The DHS S&T “Cell-All” project goal is to develop sensors that can detect life-threatening gases to be incorporated into cell phones. One feature of the Synkera MikroKera Ultra is: available with or without case.</p>	<p>A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>
<p>Synkera MikroKera Ultra module (detector case) includes a front side, a rear side, a Central Processing Unit (cpu), and a power source that is battery, USB or AC adapter.</p>	<p>a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);</p>	<p>4. The multi sensor detection and lock disabling system [of claim 1] wherein the power source for the detector case can be a battery source. (7,385,497)</p>

<p>Light-emitting diode (LED) indicators for sensor status and state of battery charge</p>	<p>a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection. (RE 43,990)</p>
<p>The Samsung Galaxy s6, GPS and internet capabilities as leverage for the Synkera MikroKera Ultra module (detector case) GPS connection and internet connection. Synkera MikroKera Ultra module (detector case) includes a power connection that is USB or AC adapter.</p>	<p>an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>

<p>Synkera is now engineering new packaging solutions that take advantage of the extremely small active area of the MikroKera Ultra sensor. We have already demonstrated a 2-sensor array on a SMT-style package (an 8-pin SOIC), and have designs for a 3-sensor array in an even smaller 3x3x1mm package. Co-packaging this design with integrated circuitry (required to capture the sensor signal) will allow for this sensor to be embedded in modern smartphones. One feature of the Synkera MikroKera Ultra is: available with or without case.</p>	<p>a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>
<p>The Samsung Galaxy s6, sound alarm indicator capabilities as leverage for the Synkera MikroKera Ultra module (detector case) sound alarm indicator. Synkera MikroKera Ultra module (detector case) includes Light-emitting diode (LED) indicators for sensor status.</p>	<p>each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;</p>	<p>29. The communication device [of claim 11] wherein the communication device has a display or LCD screen for visualization of the status of the sensors and other data reporting information. (RE 43,990)</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the Synkera MikroKera Ultra module (detector case) automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy s6, sound alarm indicator capabilities as leverage for the Synkera MikroKera Ultra module (detector case) sound alarm indicator. Synkera MikroKera Ultra module (detector case) includes Light-emitting diode (LED) indicators for sensor status. The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the Synkera MikroKera Ultra module (detector case) automatic lock disabler. After several unsuccessful log-in attempts, a Samsung device automatically locks itself up as a security feature.</p>	<p>whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.</p>	<p>37. The automatic/mechanical lock disabler system [of claim 36] wherein the automatic/mechanical lock disabler has a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear, explosive, and contraband agent or compound to include indicator lights corresponding to detecting humans, motion, temperature, shock and tampering which is capable of being disposed within the detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection. (8,106,752)</p>

"Cell-All": Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims
<p>Synkera presented the MikroKera Ultra Module at the Department of Homeland Security S&T "Cell-All" demonstration in Los Angeles on September 28, 2011. Synkera offers a general purpose digital module for evaluation and use of MikroKera Ultra chemical sensors. Synkera Technologies has been funded by DHS to develop sensors that are suitable for integration into cell phones and other ubiquitous electronic devices carried by first responders and the public at large. The DHS S&T "Cell-All" project goal is to develop sensors that can detect life-threatening gases to be incorporated into cell phones. One feature of the Synkera MikroKera Ultra is: available with or without case. The MikroKera Ultra Module is interconnected to monitoring equipment through Bluetooth communications. The monitoring equipment for this "Cell-All" project is at least a Samsung Galaxy s6 smartphone that has an Android operating system (O/S).</p>	<p>Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The Samsung Galaxy S6 capable of transmitting signals and messages to the Synkera Mikrokera Ultra Module (multi-sensor detection device).</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving signals and messages to the Synkera Mikrokera Ultra Module (multi-sensor detection device).</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the Synkera MikroKera Ultra module (detector case) automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the Synkera MikroKera Ultra module (detector case) automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy s6 is implemented: “Similarly, S&T is pursuing what’s known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. As a result, Dennis hopes to have 40 prototypes in about a year, the first of which will sniff out carbon monoxide and fire.</p>	<p>wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist...; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
---	--	--

"Cell-All": Apple iPhone	Patent #: 9,096,189; Independent Claim 8	Patents: 8,106,752; & RE 43,990; Dependent Claims
<p>The "Cell-All" initiative. The Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), Cell-All aims "to equip your cell phone with a sensor capable of detecting deadly chemicals", says Stephen Dennis, Cell-All's program manager. S&T pursued cooperative agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. Jing Li, a physical scientist at NASA's Ames Research Center, developed new technology that would bring compact, low-cost, low-power, high-speed nanosensor-based chemical sensing chip which consists of 64 nanosensors and plugs into an Apple iTouch 30-pin dock connector. The device is designed to be plugged in to an Apple iPhone to collect, process and transmit sensor data. The new device is able to detect and identify chemicals in the air using a "sample jet" and a multiple-channel silicon-based sensing chip, which consists of 64 nanosensors, and sends detection data to another phone (e.g. Apple iPhone) or a computer via telephone communication network or Wi-Fi.</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p> <p>Patent # RE43,990 specifications: Illustrated in FIGS. 1-19 is a multi-sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities... As shown in FIGS. 1-10, the multi sensor detection and lock disabling system 10 includes at least one--and preferably many--detector case 12 that can be placed in, on, upon or adjacent the product, such as... sitting upon a seaport dock or pier 20... The detector case 12 can be modified and adapted... Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case.</p>

<p>Jing Li, a physical scientist at NASA's Ames Research Center, developed new technology that would bring compact, low-cost, low-power, high-speed nanosensor-based chemical sensing chip which consists of 64 nanosensors and plugs into an ITouch 30-pin dock connector. The device is about the size of a postage stamp and is designed to be plugged in to an Apple iPhone to collect, process and transmit sensor data.</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>The device is about the size of a postage stamp and is designed to be plugged in to an iPhone to collect, process and transmit sensor data. The new device is able to detect and identify chemicals in the air using a "sample jet" and a multiple-channel silicon-based sensing chip, which consists of 64 nanosensors, and sends detection data to another phone (e.g. iPhone) or a computer via telephone communication network or Wi-Fi.</p>	<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween,</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>

<p>If the Apple Touch ID doesn't recognize your finger, you'll be asked to try again. After five failed attempts, you'll be given the option of entering your Apple ID password. In addition, you will need to enter your Apple ID password after: (1) Restarting your device, and (2) Enrolling or deleting fingers. If your device is lost or stolen, you can immediately disable Touch ID from being used to unlock your device with Find My iPhone Lost Mode. iOS 7 (or later) offers additional protection against theft with Activation Lock, which requires an Apple ID and password to turn off Find My iPhone, erase data, or reactivate your device.</p>	<p>wherein the monitoring equipment is equipped with a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (to make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. Apple uses AGPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast initial connection along with improving GPS accuracy.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom; or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>Apple iPhone to collect, process and transmit sensor data. The new device is able to detect and identify chemicals in the air using a "sample jet" and a multiple-channel silicon-based sensing chip, which consists of 64 nanosensors, and sends detection data to another phone (e.g. Apple iPhone, Apple Satellite Phone) or a computer via telephone communication network or Wi-Fi.</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>The Apple iPhone has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE, this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment; and</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Cellular carriers have precise GPS measurements of locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range and trilateration to find an area that overlaps among them. Apple uses AGPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast connection along with improving GPS accuracy.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>The Apple iPhone is implemented:</p> <p>“Similarly, S&T is pursuing what’s known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. As a result, Dennis hopes to have 40 prototypes in about a year, the first of which will sniff out carbon monoxide and fire.</p>	<p>wherein the multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist...; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	--	---

<p>The device is about the size of a postage stamp and is designed to be plugged in to an iPhone to collect, process and transmit sensor data. The new device is able to detect and identify chemicals in the air using a "sample jet" and a multiple-channel silicon-based sensing chip, which consists of 64 nanosensors, and sends detection data to another phone (e.g. iPhone) or a computer via telephone communication network or Wi-Fi.</p>	<p>wherein the multi sensor detection device for any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>Apple iPhone to collect, process and transmit sensor data. The new device is able to detect and identify chemicals in the air using a "sample jet" and a multiple-channel silicon-based sensing chip, which consists of 64 nanosensors, and sends detection data to another phone (e.g. Apple iPhone, Apple Satellite Phone) or a computer via telephone communication network or Wi-Fi.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

"Biotouch" Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>Partnership between scientists and engineers at U.S. Army Edgewood Chemical Biological Center (ECBC), iSense, LLC, U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) and the Defense Threat Reduction Agency (DTRA). ECBC, iSense, CERDEC and DTRA are working together to give warfighters a quick, new way to evaluate potential chemical/biological (CB) threats using smartphones and an encrypted network within minutes. "The idea is to have two smartphones: the Biotouch that could test the VOC and the Nett Warrior phone that would receive the information from a different location. The two will be able to communicate with each other through a phone portal within the encrypted network," explained Emanuel. VOCs are postage stamp-sized, colorimetric sensor assays with 88 different indicator dyes developed by iSense LLC (Boston, MA).</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>
<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The "Biotouch" device is the cell phone detection device.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone. The "Biotouch" device is the cell phone detection device.</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts.</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>A 122 page report focuses on the evolution of the seven wireless interfaces now found in the high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging. Smartphones today include receivers for GPS (US), GLONASS (Russia), and Beidou COMPASS (China). New regional satellite navigation systems from Japan (QZSS) and India (IRNSS) are being introduced over the coming several years. The Bluetooth Low Energy / Smart standard is migrating to the new v4.2 revision. This new personal area wireless networking standard revision enables some compelling use cases that leading smartphone OEMs are likely to rapidly adopt and deploy. Bluetooth Smart potentially has a role to play in wireless battery charging as a control and status side-channel mechanism, synergistically linking these two wireless subsystems.</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	--	---

<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>One major feature that Samsung added to its Galaxy line of smartphones was the heart rate monitor. The health-focused technology heart rate sensor is cleverly positioned on the back of the phone and embedded into the same opening as the LED flash. Samsung only allows you to register 4 fingerprints to set-up the fingerprint scanner; a security feature for easy log-in and lock-out.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

"Biotouch System" / "Nett Warrior" Smartphone System	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims
<p>The U.S. Army' developed a biological and chemical detection system. They developed volatile organic compound (VOC) strips that work with a device called a Biotouch. Biotouch relays information from VOC strips and sends results to a Nett Warrior Samsung smartphone, Defense Systems reports. Partnership between scientists and engineers at U.S. Army Edgewood Chemical Biological Center (ECBC), iSense, LLC., U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) and the Defense Threat Reduction Agency (DTRA). ECBC, iSense, CERDEC and DTRA work is to evaluate potential chemical/biological (CB) threats using smartphones. "The idea is to have two smartphones: the Biotouch that could test the VOC and the Nett Warrior phone. VOCs are postage stamp-sized, colorimetric sensor assays with 88 different indicator dyes developed by iSense LLC (Boston, MA).</p>	<p>A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>The U.S. Army developed a biological and chemical detection system. They developed volatile organic compound (VOC) strips that work with a device called a Biotouch. Biotouch relays information from VOC strips and sends results to a Nett Warrior Samsung smartphone. Partnership between scientists and engineers at U.S. Army Edgewood Chemical Biological Center (ECBC), iSense, LLC., U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) and the Defense Threat Reduction Agency (DTRA). ECBC, iSense, CERDEC and DTRA work is to evaluate potential chemical/biological (CB) threats using smartphones. "The idea is to have two smartphones: the Biotouch that could test the VOC and the Nett Warrior phone. VOCs are postage stamp-sized, colorimetric sensor assays with 88 different indicator dyes developed by iSense LLC (Boston, MA).</p>	<p>a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor";</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>
---	--	---

<p>Researchers developed volatile organic compound (VOC) strips that work with a device called a Biotouch smartphone. The device relays information from VOC strips for analysis and sends results to a Nett Warrior smartphone, a Samsung phone adapted for military use, Defense Systems reports</p>	<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>
<p>The idea is to have two smartphones: the Biotouch smartphone that could test the VOC and the Army's soldier-worn "Nett Warrior" Samsung GALAXY Note II smartphone system. VOCs are postage stamp-sized, colorimetric sensor assays with 88 different indicator dyes developed by iSense LLC (Boston, MA).</p> <p><i>Plaintiff Patent 9,096,189, Col. 14, Lines 29-36. "Product grouping 3 (detector case; modified and adapted) include, but are not limited to... detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to..."</i></p>	<p>wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>ECBC already has a device called the SmartCAR, short for "smart color-metric assay reader." That hand-held device was developed by ECBC engineer Colin Graham. The SmartCAR does not read the same color-metric assays that Miklos and Dixon are working on. The SmartCAR, in conjunction with the Nett Warrior device, can run the evaluation, capture the results, and transmit the results, along with latitude, longitude and time to a central location on an Army network so that it can be used by commanders,</p> <p>Emanuel said.</p>	<p>wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
<p>The system is a colorimetric detection assay, a swatch of paper about the size of a postage stamp that is printed with several dozen indicator chemicals arranged in a grid of small dots. Each dot is made from a differently-colored indicator chemical that will have a unique color change in response to any compound it comes in contact with: from chemical threats, to biological threats</p>	<p>a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>Researchers developed volatile organic compound (VOC) strips that work with a device called a Biotouch. The device relays information from VOC strips for analysis and sends results to a Nett Warrior smartphone, a Samsung phone adapted for military use, Defense Systems reports.. The device reads the result of chemical detection paper and transmit the results into the Army's network via the soldier-worn "Nett Warrior" smartphone system. The Nett Warrior system is a Samsung Galaxy Note II smartphone worn in a chest-mounted pouch and connected to networked radio such as a Harris Falcon III AN/PRC-152A wideband networking handheld radio or the older General Dynamics AN/PRC-154A Rifleman Radio.</p>	<p>wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.</p>	<p>108. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).</p>
--	---	---

iPhone "Biodetector" Smartphone	Patent #: 9,096,189; Independent Claim 4	Patent #: RE 43,990; Dependent Claims
<p>Pro. Brian T. Cunningham, University of Illinois has won a \$300,000 National Science Foundation grant for research into turning smartphones into biodetectors. The biodetectors used in counterterrorism fall into three broad categories: biochemical systems detecting a DNA sequence or protein unique to the bioagent through interaction with a test molecule; tissue-based systems, in which a bioagent or toxic chemical affect living mammalian cells, causing them to undergo some measurable response; and chemical mass spectrometry systems, which break samples down into their chemical components whose weights are then compared to those of known biological or chemical agents.</p>	<p>A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>The sensitivity of biodetectors allows them to be of considerable use as early detection systems against chemical or biological attacks. They are employed to monitor the environment and can respond to low concentrations of any harmful substances that may be present.</p>	<p>comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>

<p>Cunningham said the future of smartphones is to come equipped with built-in biosensors and dedicated cameras could be just a few years away. Cunningham has moved beyond the iPhone "cradle" laser pointer. Cunningham plans to use his new grant to develop a means of using the iPhone independent of the cradle, so that all of the app's capabilities can be used without any additional hardware.</p>	<p>comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>Touch ID is a fingerprint recognition feature, designed and released by Apple Inc., and is currently available on the iPhone 5S, iPhone 6, iPhone 6 Plus, iPhone 6s, iPhone 6s Plus, iPad Air 2, iPad Pro, and the iPad Mini 3 and iPad Mini 4.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>122. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>

<p>Cunningham said the future of smartphones is to come equipped with built-in biosensors and dedicated cameras could be just a few years away. A smartphone already has microphones and cameras—its ears and eyes. Installing this capability into a mobile device effectively turns it into a multipurpose sensor. “We are very interested in a simple, portable, and inexpensive instrument which can be used for early detection of cancer, HIV, and other pathogens,” said graduate student Hojeong Yu. Biosensors sensors currently exist or are being tested for their ability to detect a wide range of targets, including: gases like methane and sarin; explosives like TNT; chemicals like isopropyl alcohol; foodborne; bugs like salmonella and listeria; allergens like peanuts; water contaminants like lead and pesticides; and infectious diseases like influenza and HIV.</p>	<p>wherein the built-in embedded multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories; and</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices....; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	--

Cunningham sees this technology as applicable around the world (e.g. cellular communication; satellite communication). Doctors in remote parts of the world being able to test patients without needing expensive lab equipment because all of the devices they need are in the palms of their hands. Cunningham envisions the capability for an inexpensive, handheld biosensor instrument with web connectivity (e.g. internet) to enable point-of-care sensing in environments that have not been practical previously.

wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-long or short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for communication therebetween;

108. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).

<p>The Smartphone Biodetector is currently being implemented by the University of Illinois and the National Science Foundation “A lot of these tests require machines that cost hundreds of thousands of dollars,” Cunningham said. “We’re able to get the same results with a \$200 smartphone, which could really help in a number of different situations.” “We are very interested in a simple, portable, and inexpensive instrument which can be used for early detection of cancer, HIV, and other pathogens,” said graduate student Hojeong Yu. “Current laboratory instruments are too expensive and unwieldy to be used for home-healthcare applications and point-of-care diagnostics, and we expect the smartphone biodetection instrument to be a much more portable solution for biodetection needs in the field”</p>	<p>wherein the built-in embedded multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	---	---

"PathTracker" An iPhone-based Detection Instrument	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims
<p>National Science Foundation (NSF) to invest \$1 million in smartphone-based system for mobile disease detection. Professor Brian T. Cunningham the director of the Micro and Nanotechnology Laboratory (MNTL) and also a bioengineering professor at the University of Illinois, is the principal investigator for PathTracker: A smartphone-based system for mobile infectious disease detection and epidemiology. The PathTracker will mitigate economic losses associated with infectious disease in the horse industry; the developed technology will be equally applicable to humans, food animals, companion animals, ebola, HIV, tuberculosis, and malaria through a custom handheld detection instrument that interfaces with the back-facing camera of a conventional smartphone (e.g. iPhone)</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>The PathTracker: developed technology will be equally applicable to humans, food animals, companion animals, ebola, HIV, tuberculosis, and malaria through a custom handheld detection instrument that interfaces with the back-facing camera of a conventional smartphone (e.g. iPhone)</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>

<p>Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The results from the device can be stored in the phone and later added to a biosurveillance cloud database, allowing for an electronic archive of data that is available to anyone with access to the cloud.</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>
<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. Apple uses A-GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast initial connection along with improving GPS accuracy.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>Using SOS one-touch smartphone application, the iPhone data is relayed to the control center to include full profile of an exact, GPS based location; Digital Transmission of Distress. The control center will react to any emergency, providing two-way communication enabling real time tracking and alerting.</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>A software interface (app) running on the smartphone scans the pathogens, biomarkers or DNA and sends the data to a remote server at the control center. The servers use the data to measure the results of the scans, and return the results in a short period of time, assuming users have access to an internet connection.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>Cellular carriers have precise GPS measurements of locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range and trilateration to find an area that overlaps among them. Apple uses AGPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast connection along with improving GPS accuracy.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>

<p>A mobile device software application will guide the user through the assay process, interpret the results of the detection (including correlation of assay measurements with on-chip experimental controls), and communicate results to a cloud-based data management system along with other relevant information provided by the user. Importantly, the app will enable the user to view the results of tests performed by other users, with a mobile device interface that enables simple visualization of the locations, times, and circumstances surrounding positive/negative tests. The system will enable users to request customizable alerts when positive tests occur within the network of users</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic; combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

<p>Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The results from the device can be stored in the phone and later added to a biosurveillance cloud database, allowing for an electronic archive of data that is available to anyone with access to the cloud.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>iPhone and iPad Touch ID is a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>99. The multi-sensor detection system [of claim 81], wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.</p>
<p>Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The results from the device can be stored in the phone and later added to a biosurveillance cloud database, allowing for an electronic archive of data that is available to anyone with access to the cloud.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

Navy Marine Corps Intranet (NMCI) Network - Apple iPad	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>The Navy Marine Corps Intranet (NMCI) is the world's largest purpose-built network with more than 400,000 seats for more than 800,000 user accounts; it is also a unified, flexible and functional IT platform that has become the foundation on which the Navy and Marine Corps support their broader strategic objectives. NMCI connects Sailors, Marines and Civilians in the continental U.S., Hawaii, and Japan. Navy NMCI users may begin transitioning from BlackBerry devices to Apple and Android smartphones and tablets. NMCI users are now authorized to procure and use the iPhone 5s, iPhone 6, and iPhone 6 Plus smartphones, as well as the iPad Air and iPad Air 2 tablets with NMCI Email. All Navy organizations are to begin the contracting and transition process through their wireless account manager for iPhones and iPad service. Government furnished equipment (GFE). GFE includes laptops; smart phones; tablets; and a virtual desktop solution, such as "NMCI". Unlike GFE, personal devices cannot be integrated into the network's device management tools</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. Apple A4 is based on the ARM processor architecture. The first version released runs at 1 GHz for the iPad and contains an ARM Cortex-A8 CPU core.</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPad to connect to the internet anywhere cell phone works, to check emails.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi).</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>The Navy Marine Corps Intranet (NMCI) Network Apple iPad communication device receives signals from, and transmits signals to any of one or more products listed in any of the plurality of products grouped by common features of design similarities to include but is not limited to, stall, stop or vehicle slowdown systems; disabling lock systems; biometrics systems; near field communication systems; detection systems, and communication/monitoring devices and systems, through software application downloads, physical interfaces, gateways, processors and communication means and methods (e.g. Bluetooth; long and/or short radio frequency (RF)).</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition... ; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPad to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Apple's "Touch ID"; a fingerprint identity sensor that makes it easy to get into the iPad device. The biometric "Touch ID" is used with the iPhone 5s or later, iPad Pro, iPad Air 2, or iPad mini 3 or later. Figure 1 image from the 2008 Apple patent 20100082444 showing the 2008 Apple patent 20100082444 showing NFC Logo and fingerprint scanner (e.g., NFC + Fingerprint Scanner). The image displays the NFC Logo at the top and the Fingerprint Sensor at the bottom. The image is from published patent application 20100082444 filed on September 30, 2008 and is now patent [9,026,462] issued May 05, 2015. In this patent Apple speaks a great deal about biometrics and more directly fingerprint scanner built into the face of the illustrated Apple iPhone (#45)</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>Every iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPad to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

Navy Marine Corps Intranet (NMCI) Network - Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims
<p>The Navy Marine Corps Intranet (NMCI) is the world's largest purpose-built network with more than 400,000 seats for more than 800,000 user accounts; it is also a unified, flexible and functional IT platform that has become the foundation on which the Navy and Marine Corps support their broader strategic objectives. NMCI connects Sailors, Marines and Civilians in the continental U.S., Hawaii, and Japan. Navy NMCI users may begin transitioning from BlackBerry devices to Apple and Android smartphones and tablets. NMCI users are now authorized to procure and use the iPhone 5s, iPhone 6, and iPhone 6 Plus smartphones, as well as the iPad Air and iPad Air 2 tablets with NMCI Email. All Navy organizations are to begin the contracting and transition process through their wireless account manager for iPhones and iPad service. Government furnished equipment (GFE). GFE includes laptops; smart phones; tablets; and a virtual desktop solution, such as "NMCI". Unlike GFE, personal devices cannot be integrated into the network's device management tools</p>	<p>Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The Samsung Galaxy S6 capable of transmitting signals and messages to at least one of a multi-sensor detection device, a maritime cargo container, a cell phone detection device or any of all devices of the 400,000 seats and 800,000 user accounts that forms a plurality product group.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving signals and messages to at least a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or any of all devices of the 400,000 seats and 800,000 user accounts that forms a plurality product group.</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities: After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities: After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy s6 is implemented: . Navy Marine Corps Intranet (NMCI) connects Sailors, Marines and Civilians in the continental U.S., Hawaii, and Japan. Navy NMCI users may begin transitioning from Blackberry devices to Apple and Android smartphones and tablets. All Navy organizations are encouraged to begin the contracting and transition process through their wireless account manager. Government furnished equipment (GFE). GFE includes laptops; BlackBerry's or other smart phones; tablets; and a virtual desktop solution, such as "NMCI on a Stick."</p>	<p>wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices....; similarities in material composition...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist...; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
---	--	--

Navy Marine Corps Intranet (NMCI) Network - Samsung Galaxy s6	Patent #: 9,096,189; Independent Claim 3	Patent #: RE 43,990; Dependent Claims
<p>The Navy Marine Corps Intranet (NMCI) is the world's largest purpose-built network with more than 400,000 seats for more than 800,000 user accounts; it is also a unified, flexible and functional IT platform that has become the foundation on which the Navy and Marine Corps support their broader strategic objectives. NMCI connects Sailors, Marines and Civilians in the continental U.S., Hawaii, and Japan. Navy NMCI users may begin transitioning from BlackBerry devices to Apple and Android smartphones and tablets. NMCI users are now authorized to procure and use the iPhone 5s, iPhone 6, and iPhone 6 Plus smartphones, as well as the iPad Air and iPad Air 2 tablets with NMCI Email. All Navy organizations are to begin the contracting and transition process through their wireless account manager for iPhones and iPad service. Government furnished equipment (GFE). GFE includes laptops; smart phones; tablets; and a virtual desktop solution, such as "NMCI". Unlike GFE, personal devices cannot be integrated into the network's device management tools</p>	<p>Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and any of a plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The NMCI 400,000 seats and 800,000 user accounts leveraging the Galaxy's locking, unlocking, and disabling lock capabilities.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone. The NMCI 400,000 seats and 800,000 user accounts leveraging the Galaxy's locking, unlocking, and disabling lock capabilities.</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality of product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Once an individual phone gathers data, the information could be uploaded to wireless networks and combined with sensor data from other phones, allowing coverage of very large areas. The researchers are also seeking to integrate Bluetooth technology to expand its range beyond 5 cm (2 in). Samsung Galaxy s6 WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency (RF) connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone.</p>	<p>whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Once an individual phone gathers data, the information could be uploaded to wireless networks and combined with sensor data from other phones, allowing coverage of very large areas. The researchers are also seeking to integrate Bluetooth technology to expand its range beyond 5 cm (2 in). Samsung Galaxy s6 WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency (RF) connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
--	--	---

<p>Samsung Semiconductor now supplies the RF and Secure Element content for the Galaxy S6. Apple uses AMS RF and NXP's Secure Element components in the iPhone 6. Qualcomm has recently announced a cooperation agreement with NXP to extend both companies' NFC ecosystems. E.JL</p> <p>Wireless Research expects that the competition among Samsung, Apple, NXP and Qualcomm for NFC RF and Secure Element design wins in 2016 smartphones will intensify, leaving little opportunity for smaller suppliers such as AMS. Figure 1 image from the 2008 Apple patent 20100082444 showing NFC Logo and fingerprint scanner (e.g., NFC + Fingerprint Scanner). The image displays the NFC Logo at the top and the Fingerprint Sensor at the bottom. The image is from published patent application 20100082444 filed on September 30, 2008 and is now patent [9,026,462] issued May 05, 2015. In this patent Apple speaks a great deal about biometrics and more directly fingerprint scanner built into the face of the illustrated iPhone (#45).</p>	<p>at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency (RF) connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
--	--	---

FLIR: identiFINDER R300 / Smartphone System	Patent #: 9,096,189; Independent Claim 4	Patent #: RE 43,990; Dependent Claims
<p>FLIR Systems, Inc. announced on June 16, 2011 that the Defense Threat Reduction Agency (DTRA) has awarded it a \$1.1 million contract for a multi-year, multi-phase research and development contract to develop a mobile, ruggedized stand-off radiation detection system with identification capabilities. "FLIR has developed a radiation detection and identification device and is manufacturing the world's leading handheld radio-isotope identifier, the identiFINDER," said William Sundermeier, president of FLIR Detection and Protection. In particular, the FLIR identiFINDER R300 will identify threat objects. A threat object is radioactive material whose signature is that of material used for terrorist purposes. Threat materials are usually those used in a nuclear explosive devices or in Radiological Dispersive Devices ("Dirty" bombs). The device qualifies as a detector case with features of multiple sensors, internet and GPS connection.</p>	<p>A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p> <p>Patent # RE43,990 specifications: Illustrated in FIGS. 1-19 is a multi-sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities... As shown in FIGS. 1-10, the multi sensor detection and lock disabling system 10 includes at least one--and preferably many--detector case 12 that can be placed in, on, upon or adjacent the product, such as... sitting upon a seaport dock or pier 20... The detector case 12 can be modified and adapted... Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case.</p>

<p>The FLIR identiFINDER R300 will identify threat objects. A threat object is radioactive material whose signature is that of material used for terrorist purposes. Threat materials are usually those used in a nuclear explosive devices or in Radiological Dispersive Devices (“Dirty” bombs). Capabilities include: Automatic identification of radionuclides by analysis of gamma ray spectra and neutron detection (available only for variants equipped with a neutron detector.) The FLIR identiFINDER R300 combines the capabilities of a Personal Radiation Detector (PRD) with the radionuclide identification capabilities of a Radio-Isotope Identification Detector (RIID) into one conveniently small package. (about the size of a cell phone and is belt wearable). The device qualifies as a detector case with features of multiple sensors, internet and GPS connection.</p>	<p>comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
---	---	--

<p>FLIR's product line now offers enhanced communications allowing for the use of "One Touch Reachback". This feature allows a user to transmit data from the field through off the shelf cell phones. "In our initial partnerships with Apple, Samsung and BlackBerry, we're releasing at least interim approvals at the same time the products are commercially released," Mark Orndorff, the Defense Information Systems Agency (DISA) Mission Assurance Executive, said. "We've got the process well-greased, so when the Apple iPhone 6 was released, it was also available to the Department of Defense. We've been able to do the same with Samsung and BlackBerry." The sensor likely to be integrated in other handheld or wearable devices.</p>	<p>comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
---	--	--

<p>Apple Touch ID is a fingerprint recognition feature, designed and released by Apple Inc., and is currently available on the iPhone 5S, iPhone 6, iPhone 6 Plus, iPhone 6s, iPhone 5S, Plus, iPad Air 2, iPad Pro, and the iPad Mini 3 and iPad Mini 4.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>122. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
---	--	--

<p>FLIR has implemented a web INTERFACE in every handheld product. Users use their standard web browsing software such as Internet Explorer, Mozilla Firefox, and others. The internal software can be accessed from any PC. The device contains a driver for communicating directly over a standard USB cable eliminating a dedicated PC or outside internet connection. The ability to save and load user configured settings, operate the instrument via the PC, or download and view saved spectra and screenshots. The "One Touch Reachback" feature immediately provides full spectroscopic data, time, and GPS location with the push of a button. Through a simple Bluetooth® connection, notifications are all but automatic. "In our initial partnerships with Apple, Samsung and BlackBerry, we're releasing at least interim approvals at the same time the products are commercially released," Mark Orndorff, the Defense Information Systems Agency (DISA) Mission Assurance Executive,</p>	<p>wherein the built-in embedded multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories; and</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	---	---

<p>If the FLIR identifier R300 detects radiation above certain thresholds you can specify, it raises an alarm. Alarms can be reported via several annunciators: (e.g. product to product; product to smartphone; product to computer PC). Main Display: Details of the alarm are always displayed on-screen. Status Bar: The alarm and warning information is shown in the status bar along the display's top edge. LED: LEDs flash in several patterns. Beeper: The beeper emits various sound patterns. Vibrator: The vibrator shakes the instrument. All alarms are stored in the FLIR identifier R300's database, including date and time and GPS coordinates.</p>	<p>wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-long or short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for communication therebetween;</p>	<p>108. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).</p>
--	--	---

<p>William Sundermeier, president of FLIR Detection and Protection said, “The resulting system will provide a stand-off solution to the challenge of locating and identifying radioactive sources in field environments such as ports, maritime environments, and battlefields.” “In our initial partnerships with Apple, Samsung and BlackBerry, we’re releasing at least interim approvals at the same time the products are commercially released,” Mark Orndorff, the Defense Information Systems Agency (DISA) Mission Assurance Executive. The FLIR identIFINDER R300 combines the capabilities of a Personal Radiation Detector (PRD) with the radionuclide identification capabilities of a Radio-Isotope Identification Detector (RIID) into one conveniently small package.</p>	<p>wherein the built-in embedded multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

AOptix Stratus MX Peripheral for the Apple (iPhone) Smartphone	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims
<p>The biometrics company AOptix announced on Wednesday, February 13, 2013 that the Pentagon has awarded it, along with CACI International Inc., a \$3 million research contract to develop AOptix's Smart Mobile Identity devices for the US Department of Defense. As Wired reported, a hardware peripheral and software suite that turns a regular Apple iPhone smartphone into a device that scans and transmits data at distances not possible for current scanning technology. AOptix's hardware is a peripheral that wraps around a smartphone, so that it can record biometric data. AOptix executive Joey Pritikin told Wired, "this new gadget will be able to scan faces at up to two meters away, irises from one meter, and voice from within a typical distance from a phone. Thumbprints will still require scanning against the phone's glass face". Biometrics, also known as biostatistics or biometry, in biology, the development and application of statistical and mathematical methods to the analysis of data resulting from biological observations and phenomena.</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p> <p>Patent # RE43,990 specifications: Illustrated in FIGS. 1-19 is a multi-sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities... As shown in FIGS. 1-10, the multi sensor detection and lock disabling system 10 includes at least one--and preferably many--detector case 12 that can be placed in, on, upon or adjacent the product, such as... sitting upon a seaport dock or pier 20... The detector case 12 can be modified and adapted... Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case.</p>

<p>April 9, 2013 - AOptix unveiled the AOPtix Stratus, a mobile identity solution designed for the Apple iPhone. Featuring fingerprint, iris, voice and face recognition, the Stratus is a hardware peripheral, the Stratus MX, which houses the Apple iPhone and contains a fingerprint sensor and an AOPtix iris imaging system. Using the iPhone camera to capture faces and voice signatures, there's an extra camera for iris scanning and a small embedded fingerprint sensor. The OPtix Stratus App may be used in conjunction with AOptix Stratus MX for iris, face, fingerprint and voice biometric capture. In addition, it may be used independently off the iPhone for face and voice capture.</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>The Aptix Stratus MX turns smartphone into handheld biometric capture device. The iPhone smartphone AOptix Stratus may be used in conjunction with AOptix Stratus MX for iris, face, fingerprint and voice biometric capture. In addition, it may be used independently off the iPhone for face and voice capture.</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>

<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. Apple uses A-GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast initial connection along with improving GPS accuracy.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
<p>Using SOS one-touch smartphone application, the iPhone data is relayed to the control center to include full profile of an exact, GPS based location; Digital Transmission of Distress. The control center will react to any emergency, providing two-way communication enabling real time tracking and alerting.</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>The user inserts the iPhone in the device, plugging it in using the 30-pin connector, and then launches the app. The app interface is user-friendly and simple, and lets the user register the biometrics of the person in front of him with relative ease. Using an iPhone also lets the app register GPS coordinates and transmit all the data through the phone's mobile Internet connection.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

<p>Cellular carriers have precise GPS measurements of locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range and trilateration to find an area that overlaps among them. Apple uses A GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast connection along with improving GPS accuracy.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
--	---	--

<p>Chuck Yort, Vice President and General Manager of Identity Solutions at AOptix said. “We’ve received a great deal of interest from law enforcement and border control, national and civil ID programs, and defense. We anticipate AOptix Stratus will be embraced by healthcare, disaster relief, humanitarian aid and other areas where identity verification is essential”. Using the iPhone camera to capture faces and voice signatures, there’s an extra camera for iris scanning and a small embedded fingerprint sensor. The OPTix Stratus App may be used in conjunction with AOptix Stratus MX for iris, face, fingerprint and voice biometric capture.</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	---	---

<p>The user inserts the iPhone in the device, plugging it in using the 30-pin connector, and then launches the app. The app interface is user-friendly and simple, and lets the user register the biometrics of the person in front of him with relative ease. Using an iPhone also lets the app register GPS coordinates and transmit all the data through the phone's mobile Internet connection.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The AOptix Stratus leverages the iPhone as a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>99. The multi-sensor detection system [of claim 81], wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.</p>
<p>The user inserts the iPhone in the device, plugging it in using the 30-pin connector, and then launches the app. The app interface is user-friendly and simple, and lets the user register the biometrics of the person in front of him with relative ease. Using an iPhone also lets the app register GPS coordinates and transmit all the data through the phone's mobile Internet connection.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

MultiRae Pro Wireless Portable Multi Threat Radiation and Chemical Detector	Patent #: 9,096,189; Independent Claim 5	Patent #: RE 43,990; Dependent Claims
<p>RAE Systems was awarded a five-year contract by the Environmental Protection Agency (EPA) for its MultiRAE Pro monitors. The Federal Emergency Management Agency (FEMA) has also adopted the MultiRAE Pro monitor to its Urban Search and Rescue (US&R) equipment cache. Description: The RAE Systems MultiRAE Pro is a CBRN multithread detection tool that combines continuous monitoring capabilities for radiation and combustible gases. The MultiRAE Pro can be configured with 33 intelligent sensors to fully meet the monitoring needs of applications such as HazMat response, CBRN/TIC/TIM detection, EOD, homeland security, and civil defense. Mission: The MultiRAE Pro provides a handheld multi-gas sensor with 5 sensor channels that can detect toxic or hazardous vapors: Users; US Marine Corps. The MultiRae Pro qualifies as a multi sensor detector case that has interchangeable sensors; a battery power source; an internet connection, and, a GPS connection.</p>	<p>A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>

<p>The MultiRAE Pro Portable Multi-Threat Monitor can be easily configured to detect and monitor more than 300 volatile organic compounds (VOCs), gamma radiation, 55 combustible gases and vapors, and 25 specific toxic gases – up to six threats at a time – all in a single, highly versatile monitor. The MultiRAe Pro qualifies as a multi sensor detector case that has interchangeable sensors; a battery power source; an internet connection, and, a GPS connection.</p>	<p>a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>
<p>The ProRAE Guardian System wirelessly delivers real-time personal and point threat-detection data on toxic gases and radiation, worker/responders' location and physiological condition. It provides situational awareness, tracks and identifies toxic chemicals, radiation, and plumes. ProRAE Guardian integrates instrument data and alarm status from up to 512 RAE Systems toxic gas and radiation monitors and select third-party devices on a single dynamic map, and allows the information to be shared by multiple plant managers or responder teams through a secure Internet connection. The real-time data can be viewed remotely on a PC, smartphone or tablet.</p>	<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;</p>	<p>79. The built-in, embedded multi sensor detection system [of claim 74] wherein the product includes at least one of a built-in, embedded wireless and/or wired communication connection capable of sending signals and messages to a product; receiving signals and messages from a product; interconnected to at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation, monitoring site or another product comprises a built-in, embedded wireless and/or wired communication connection.</p>

<p>The RAE Systems MultiRAE Pro is a handheld CBRN multithread detection tool that combines continuous monitoring capabilities for radiation and combustible gases. The handheld MultiRAE Pro can be configured with 33 intelligent sensors to fully meet the monitoring needs of applications such as HazMat response, CBRN/TIC/TIM detection, EOD, homeland security, and civil defense. Mission: The MultiRAE Pro provides a handheld multi-gas sensor with 5 sensor channels that can detect toxic or hazardous vapors: Users: US Marine Corps. The MultiRae Pro handheld qualifies as a multi sensor detector case that has interchangeable sensors; a battery power source; an internet connection, and, a GPS connection.</p>	<p>wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>79. The built-in, embedded multi sensor detection system [of claim 74] wherein the product includes at least one of a built-in, embedded wireless and/or wired communication connection capable of sending signals and messages to a product; receiving signals and messages from a product; interconnected to at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation, monitoring site or another product comprises a built-in, embedded wireless and/or wired communication connection.</p>
--	---	---

<p>RAE Systems was awarded a five-year contract by the Environmental Protection Agency (EPA) for its MultiRAE Pro monitors. The Federal Emergency Management Agency (FEMA) has also adopted the MultiRAE Pro monitor to its Urban Search and Rescue (US&R) equipment cache. The handheld MultiRAE Pro can be configured with 33 intelligent sensors to fully meet the monitoring needs of applications such as HazMat response, CBRN/TTC/TIM detection, EOD, homeland security, and civil defense. The MultiRAE Pro provides a handheld multi-gas sensor with 5 sensor channels that can detect toxic or hazardous vapors: Users; US Marine Corps. MultiRAE monitors provide both personal- and point-detection capabilities for a broad range of applications, including military, homeland security, and industrial safety and industrial hygiene.</p>	<p>wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	---	--

<p>EchoView Host Mini-Controller: The EchoView Host is a mini-controller that creates a self-contained intelligent wireless network for the MultiRae Pro that supports up to 8 monitors. The easy-to-read display allows connected devices' names to be customized for easy identification of the real-time readings. The EchoView Host provides immediate remote notification of alarm conditions to keep workers informed, connected and protected. Key Feature: Bright-red high-visibility alarm lights</p>	<p>a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection.</p>
--	---	---

<p>EchoView Host Mini-Controller: The EchoView Host is a mini-controller that creates a self-contained intelligent wireless network for the MultiRae Pro that supports up to 8 monitors. Rae Systems BioHarness biometric device. This lightweight, wearable monitor measures personal vital statistics such as heart rate, body temperature, breathing rate, and posture. When connected to a RAELink3 portable wireless transmitter and the centralized ProRAE Guardian software, the BioHarness provides real-time location information and wireless awareness of the health status of responders and workers. The RAE Systems ProRAE Guardian Real-time Wireless Safety System supports the MultiRAE multi-threat detectors. The wireless applications are: Near-field communication (NFC); Bluetooth; Wi-Fi; and Mesh Networks. Worker biometric and GPS data from anywhere in the world.</p>	<p>wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.</p>	<p>78. The built-in, embedded multi sensor detection system [of claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.</p>
--	---	--

PositiveID - Boeing / "M-Band" Apple (iPhone) Smartphone	Patent #: 9,096,189; Independent Claim 7	Patent #: RE 43,990; Dependent Claims
<p>PositiveID's (PSID) M-BAND was developed by the Company's MicroFluidic Systems ("MFS") subsidiary, which received funding in excess of \$30 million from the Department of Homeland Security (DHS). M-BAND is positioned to capitalize on BioWatch Generation 3, the U.S. Government's \$3.1 billion program to detect the release of pathogens into the air as part of a defense against potential terrorist attacks on major American cities. In Dec. 2012, PSID entered into an exclusive license agreement with The Boeing Company ("Boeing"). Boeing paid PSID \$2.5 million; exclusive distributor of M-BAND for BioWatch Gen-3. M-Band is a bio-aerosol monitor with fully integrated systems for sample collection, processing and detection modules that continuously analyze air samples for the detection of bacteria, viruses, and toxins and transmit the results to smartphones (e.g. Apple iPhone), or other devices, every three hours.</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p> <p>Patent # RE43,990 specifications: Illustrated in FIGS. 1-19 is a multi-sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities... As shown in FIGS. 1-10, the multi sensor detection and lock disabling system 10 includes at least one--and preferably many--detector case 12 that can be placed in, on, upon or adjacent the product, such as... sitting upon a seaport dock or pier 20... The detector case 12 can be modified and adapted... Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case.</p>

<p>Lyle Probst, PositivellD's president, said the M-BAND can deliver results to a smartphone (e.g. Apple iPhone) and other devices every three hours. There are two potentially dangerous classifications of bio-hazards: pathogens and toxins. They require different processes. Pathogens are living organisms, and toxins are nonliving. M-BAND has modules that can be separately swapped out or maintained for each of them. The genetic sequence automatically examine the dangerous pathogens for anthrax, plague or even non-weaponized influenza. It also has the ability to detect three different toxins such as ricin, with the room to expand to four, if needed, Probst said.</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>	<p>118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.</p>
<p>Lyle Probst, PositivellD's president, said the M-BAND can deliver results to a smartphone (e.g. Apple iPhone) and other devices every three hours. There are two potentially dangerous classifications of bio-hazards: pathogens and toxins. Results are reported via a secure wireless network in real time to give an accurate and up to date status for fielded instruments.</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>	<p>17. The communication device [of claim 11] wherein the communication device has monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween.</p>

<p>Cellular carriers have extremely precise GPS measurements of the locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range—which may be dozens—and trilateration to find an area that overlaps among them. Apple uses AGPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast initial connection along with improving GPS accuracy.</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
<p>Using SOS one-touch smartphone application, the iPhone data is relayed to the control center to include full profile of an exact, GPS based location; Digital Transmission of Distress. The control center will react to any emergency, providing two-way communication enabling real time tracking and alerting.</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Using an iPhone lets an app register GPS coordinates and transmit all the data through the phone's mobile Internet connection.</p>	<p>at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

<p>Cellular carriers have precise GPS measurements of locations of all their towers. With a database of such towers, you can take measurements of the signal strength of those within range and trilateration to find an area that overlaps among them. Apple uses A-GPS for native GPS-lock improvements, and Wi-Fi network and cell tower locations are additional factors in providing a fast connection along with improving GPS accuracy.</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>	<p>92. The multi-sensor detection system [of claim 81], further comprising a global positioning system (GPS) receiver adapted for communication with at least one satellite.</p>
--	---	--

<p>Lyle Probst, PositivellD's president, said the M-BAND can deliver results to a smartphone (e.g. Apple iPhone) and other devices every three hours. There are two potentially dangerous classifications of bio-hazards: pathogens and toxins. They require different processes. Pathogens are living organisms, and toxins are nonliving. M-BAND has modules that can be separately swapped out or maintained for each of them. The genetic sequence automatically examine the dangerous pathogens for anthrax, plague or even non-weaponized influenza. It also has the ability to detect three different toxins such as ricin, with the room to expand to four, if needed, Probst said. Results are reported via a secure wireless network in real time to give an accurate and up to date status for fielded instruments.</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	---	---

<p>Using an iPhone lets the app register GPS coordinates and transmit all the data through the phone's mobile Internet connection.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The PositiveliD leverages the iPhone as a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>99. The multi-sensor detection system [of claim 81], wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.</p>
<p>Using an iPhone also lets the app register GPS coordinates and transmit all the data through the phone's mobile Internet connection.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>

PositivID / "Firefly DX" Samsung Galaxy s6 Smartphone	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>PositivID's (PSID) M-BAND developed by MicroFluidic Systems ("MFS") subsidiary; received funding excess of \$30 million from Department of Homeland Security (DHS). Firefly Dx, builds upon technology advances achieved in development of M-BAND system. Firefly Dx overview: Miniaturized version of M-BAND using same technologies, real-time PCR detection: Hand-held detection provides sample purification and biological analysis; A two-part device consisting of a portable handheld instrument with wireless communication and disposable single-use cartridges all analytical elements;</p> <p>Data processed in real time and communicated to PC or smartphone (e.g., Galaxy s6) using mobile applications and cloud storage; Has the ability to detect and identify common pathogens and diseases as various strains of influenza, E.coli, MRSA and human papilloma virus ("HPV").</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. Also the combined three-part system: a wireless portable handheld instrument; disposable single-use cartridge; and, the "Firefly DX" equals a cell-phone detection device for transmitting.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving a signal from the factory to reset (unlock) the phone. Also the combined three-part system: a wireless portable handheld instrument; disposable single-use cartridge; and, the "Firefly DX" equals a cell-phone detection device for receiving.</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot, Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces found in the Samsung Galaxy S6 smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Galaxy is interconnected to the "Firefly DX" multi-sensor detection system for activation or deactivation.</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>A 122 page report focuses on the evolution of the seven wireless interfaces now found in the high-end Samsung Galaxy s6 smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging. Smartphones today include receivers for GPS (US), GLONASS (Russia), and Beidou COMPASS (China). New regional satellite navigation systems from Japan (QZSS) and India (IRNSS) are being introduced over the coming several years. The Bluetooth Low Energy / Smart standard is migrating to the new v4.2 revision. This new personal area wireless networking standard revision enables some compelling use cases that leading smartphone OEMs are likely to rapidly adopt and deploy. Bluetooth Smartphones potentially has a role to play in wireless battery charging as a control and status side-channel mechanism, synergistically linking these two wireless subsystems.</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
--	--	---

<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>One major feature that Samsung added to its Galaxy line of smartphones was the heart rate monitor. The health-focused technology heart rate sensor is cleverly positioned on the back of the phone and embedded into the same opening as the LED flash. Samsung only allows you to register 4 fingerprints to set-up the fingerprint scanner; a security feature for easy log-in and lock-out.</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

2"x2" Detection Device (DD) Samsung Galaxy s6 Smartphone	Patent #: 7,385,497; Independent Claim 1	Patents: 7,385,497; 8,106,752; & RE 43,990; Dependent Claims
<p>In response to the Domestic Nuclear Detection Office's (DNDO) BAA 09-102 Passport Systems, Inc. of Billerica, MA has developed a system of networked portable spectroscopic radiation detectors to improve the detection, localization, and identification of radiological threats. The Intelligent Radiation Sensor Systems (IRSS) 2"x2" Detection Device (DD) comprises: a Standard Interface; an Individual Radiation Detection Device (IRDD); and, an Android smartphone (including GPS). The Detector Augmentation Device (DAD) was implemented by leveraging existing Android smartphone technology, and it provides all the functionality to interface with the IRDD and the operational user through an appropriate, configurable GUI. The DAD also provides a platform for all the communications and computation. The DAD is responsible for establishing and maintaining a robust ad hoc network. This is accomplished using the native WiFi (IEEE 802.11b) capability on the smartphone and open source mesh network applications.</p>	<p>A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>

<p>The IRDD consists of COTS and OEM components – including signal processing electronics, HV supply, battery, photo-multiplier tube, and scintillator crystal – that were integrated into a modular, portable system. The significant computations required by the advanced algorithms, were all carried out on the smartphone processor.</p>	<p>a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);</p>	<p>4. The multi sensor detection and lock disabling system [of claim 1] wherein the power source for the detector case can be a battery source. (7,385,497)</p>
<p>Figure 8: Detection confidence for networked and non-networked detectors for a very weak moving source. The red line is the average detection metric with the source present. The blue lines are source absent trials. The dashed red lines indicate ± 1 standard deviation.</p> <p>Figure 9: Live tracking experiment of a Co source. Green circles are detectors. Blue dots are source position hypotheses. The red circle is the estimated source position and the white ellipse represents the positional uncertainty.</p>	<p>a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection. (RE 43,990)</p>
<p>The Samsung Galaxy s6, GPS and internet capabilities as leverage for the Passport Systems 2"x2" Detection Device (detector case) GPS connection and internet connection. The hardware integration concept is leveraging "smartphones" for computation and communications; utilizing integrated differential GPS when possible.</p>	<p>an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>

<p>The detection device (DD) is a key system element of IRSS and, is comprised of two parts: 1) the detector augmentation device (DAD) and 2) the individual radiation detection device (IRDD). The two devices are loosely coupled to maintain flexibility and upgradability. This modular design philosophy allows for plug-and-play of various sensors with unique characteristics (e.g. sensitivity and spectroscopic resolution) depending on operator need and component availability.</p>	<p>a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>
<p>The Samsung Galaxy s6, sound alarm indicator capabilities as leverage for the 2"x2" Detection Device (detector case) sound alarm indicator. The 2"x2" Detection Device(detector case) includes Light-emitting diode (LED) indicators for sensor status.</p>	<p>each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;</p>	<p>29. The communication device [of claim 11] wherein the communication device has a display or LCD screen for visualization of the status of the sensors and other data reporting information. (RE 43,990)</p>
<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the the 2"x2" Detection Device (detector case) automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>

<p>The Samsung Galaxy s6, sound alarm indicator capabilities as leverage for the the 2"x2" Detection Device (detector case) sound alarm indicator. The 2"x2" Detection Device (detector case) includes Light-emitting diode (LED) indicators for sensor status. The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the the 2"x2" Detection Device (detector case) automatic lock disabler. After several unsuccessful log-in attempts, a Samsung device automatically locks itself up as a security feature.</p>	<p>whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.</p>	<p>37. The automatic/mechanical lock disabler system [of claim 36] wherein the automatic/mechanical lock disabler has a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear, explosive, and contraband agent or compound to include indicator lights corresponding to detecting humans, motion, temperature, shock and tampering which is capable of being disposed within the detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection. (8,106,752)</p>
---	---	---

1"x2" Detection Device (DD) Samsung Galaxy s6 Smartphone	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims
<p>In response to the Domestic Nuclear Detection Office's (DNDO) BAA 09-102 Passport Systems, Inc. of Billerica, MA has developed a system of networked portable spectroscopic radiation detectors to improve the detection, localization, and identification of radiological threats. The Intelligent Radiation Sensor Systems (IRSS) 1"x2" Detection Device (DD) comprises: a Standard Interface; an Individual Radiation Detection Device (IRDD); and, an Android smartphone (including GPS). The Detector Augmentation Device (DAD) was implemented by leveraging existing Android smartphone technology, and it provides all the functionality to interface with the IRDD and the operational user through an appropriate, configurable GUI. The DAD also provides a platform for all the communications and computation. The DAD is responsible for establishing and maintaining a robust ad hoc network. This is accomplished using the native WiFi (IEEE 802.11b) capability on the smartphone and open source mesh network applications.</p>	<p>Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The Samsung Galaxy S6 capable of transmitting signals and messages to the 1"x2" Detection Device (DD) comprises: a Standard Interface; an Individual Radiation Detection Device (IRDD); and, an Android smartphone (including GPS).</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving signals and messages to the 1"x2" Detection Device (DD) comprises: a Standard Interface; an Individual Radiation Detection Device (IRDD); and, an Android smartphone (including GPS).</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the Individual Radiation Detection Device (IRDD) automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the Individual Radiation Detection Device (IRDD) automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy s6 is implemented: "Similarly, S&T is pursuing what's known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. As a result, Dennis hopes to have 40 prototypes in about a year, the first of which will sniff out carbon monoxide and fire.</p>	<p>wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist...; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
---	--	--

<p>Nets² SmartShield G300 Radiation Detector Samsung Galaxy s6 Smartphone</p>	<p>Patent #: 7,385,497; Independent Claim 1</p>	<p>Patents: 7,385,497; 8,106,752; & RE 43,990; Dependent Claims</p>
<p>Passport Systems Inc. G300 Radiation Detector alarms when radiation levels are detected; used as a standalone device or as part of a network; is the same size, form factor and weight as a smartphone and easily added to the belt of safety personnel; is paired with a smartphone via Bluetooth, and automatically joins a SmartShield Network.</p> <p>The Network Sensor System (Nets²) SmartShield G300 Radiation Detector is designed specifically for the DHS Securing-the-Cities initiative and Human Portable Tripwire program. Passport Systems, in response to the US Department of Homeland Security (DHS) needs, developed a compact and scalable radiation detector system, the Nets² SmartShield. The smartphone is integral to the advanced features of the SmartShield system. It provides an advanced user interface, a computer to handle advanced identification, geolocation, and data fusion algorithms, and an integrated communications platform to complete reachback as well as data collaboration functions.</p>	<p>A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>

<p>G300 Detector: Power Source Battery: Integrated, Rechargeable Li-Ion (Micro-USB 2.0 recharging port; up to 700 recharge cycles). Operating Period: 60+ hours (continuous) in surveillance mode</p>	<p>a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);</p>	<p>4. The multi sensor detection and lock disabling system [of claim 1] wherein the power source for the detector case can be a battery source. (7,385,497)</p>
<p>Samsung Galaxy s6 Smartphone: Touchscreen color display when synced with detector. The SmartShield System detected and located a sample source efficiently and accurately. The blue coloring depicts the level of natural background radiation collected automatically by the system. The icons on the Passport Systems, Inc. screen represent blue force detectors and the radiation symbol indicates the detection of a check source. The BCU shows 16 fixed detectors represented by the different colored diamond shapes.</p>	<p>a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;</p>	<p>119. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear explosive and contraband agent or compound which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection. (RE 43,990)</p>
<p>The Samsung Galaxy s6 smartphone provides communications with the detector, real-time communications to a reachback server, a computational platform, GPS based localization, storage of local data, as well as a user interface which provides network information through hosted server software. The Server software can be run on any standard computer and is typically offered in a Cloud environment</p>	<p>an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>

<p>The system as currently delivered performs mirrored computations at every node. In other words, all computing devices including the smartphone and BCU, perform Data Fusion and isotope identification simultaneously and can work independently if need be. If one node drops out all other nodes continue to operate. The architecture of the SmartShield NetS2 system is an open platform that considers communications and computing devices to be independent from each other.</p>	<p>a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;</p>	<p>2. The multi sensor detection and lock disabling system [of claim 1] wherein each detector is capable of being utilized as a stand-alone scanner for detecting the chemical, biological and radiological agents and compounds. (7,385,497)</p>
<p>The Samsung Galaxy s6, sound alarm indicator capabilities as leverage for the NetS² SmartShield G300 Radiation Detector sound alarm indicator. The 2"x2" Detection Device(detector case) includes Light-emitting diode (LED) indicators for sensor status.</p>	<p>each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;</p>	<p>29. The communication device [of claim 11] wherein the communication device has a display or LCD screen for visualization of the status of the sensors and other data reporting information. (RE 43,990)</p>
<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the the NetS² SmartShield G300 Radiation Detector automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>

<p>The Samsung Galaxy s6, sound alarm indicator capabilities as leverage for the the Nets² SmartShield G300 Radiation Detector sound alarm indicator. The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the the Nets² SmartShield G300 Radiation Detector automatic lock disabler. After several unsuccessful log-in attempts, a Samsung device automatically locks itself up as a security feature.</p>	<p>whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.</p>	<p>37. The automatic/mechanical lock disabler system [of claim 36] wherein the automatic/mechanical lock disabler has a plurality of indicator lights with each indicator light corresponding to one chemical, biological, radiological, nuclear, explosive, and contraband agent or compound to include indicator lights corresponding to detecting humans, motion, temperature, shock and tampering which is capable of being disposed within the detector case and lighting up upon detection of that specific agent or compound for providing visual confirmation of the detection. (8,106,752)</p>
--	---	---

Nets² SmartShield G500 Radiation Detector Samsung Galaxy s6 Smartphone	Patent #: 9,096,189; Independent Claim 2	Patents: 8,106,752; & RE 43,990; Dependent Claims
<p>Passport Systems Inc. G500 Radiation Detector alarms when radiation levels are detected; used as a standalone device or as part of a network; is the same size, form factor and weight as a smartphone and easily added to the belt of safety personnel; is paired with a smartphone via Bluetooth, and automatically joins a SmartShield Network.</p> <p>The Network Sensor System (Nets²) SmartShield G500 Radiation Detector is designed specifically for the DHS Securing-the-Cities initiative and Human Portable Tripwire program. Passport Systems, in response to the US Department of Homeland Security (DHS) needs, developed a compact and scalable radiation detector system, the Nets² SmartShield. The smartphone is integral to the advanced features of the SmartShield system. It provides an advanced user interface, a computer to handle advanced identification, geolocation, and data fusion algorithms, and an integrated communications platform to complete reachback as well as data collaboration functions.</p>	<p>Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. Modern microprocessors appear in everything from automobiles to mobile phones. Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>The Samsung Galaxy S6 capable of transmitting signals and messages to the NetS² SmartShield G500 Radiation Detector (multi-sensor detection device) .</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>The Samsung Galaxy S6 capable of receiving signals and messages to the NetS² SmartShield G500 Radiation Detector (multi-sensor detection device)</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the NetS² SmartShield G500 Radiation Detector automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging</p>	<p>monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>

<p>The Samsung Galaxy s6, automatic lock disabler capabilities as leverage for the NetS² SmartShield G500 Radiation Detector automatic lock disabler. After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If the user is unable to log in to the phone after doing all the available security layers, there's no other option left for the user to do but to have the phone unlocked.</p>	<p>whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>34. The automatic/mechanical lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals. (8,106,752)</p>
<p>The Samsung Galaxy s6 is implemented: “Similarly, S&T is pursuing what's known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. As a result, Dennis hopes to have 40 prototypes in about a year, the first of which will sniff out carbon monoxide and fire.</p>	<p>wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>124. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of: sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices...; similarities in material composition...; similarities in security problems of at least one of: theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist...; grouping security devices to form a network of ubiquitous sensing and detecting.</p>

<p>The Samsung Galaxy S6: WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE, apt-X</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
---	--	--

"TOUGHBOOK 31" Laptop Passport Systems Inc. Base Control Unit (BCU)	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>The Passport Systems "Base Control Unit" (BCU) is implemented using the Panasonic Toughbook ruggedized laptop, and in response to the Domestic Nuclear Detection Office's (DNDO) BAA 09-102 Passport Systems, Inc. has developed a system of networked portable spectroscopic radiation detectors to improve the detection, and identification of radiological threats. The Intelligent Radiation Sensor Systems (IRSS) 1"x2" and 2"x2" Detection Devices (DD).</p> <p>The Network Sensor System (Nets²) SmartShield G300 and G500 Radiation Detectors are designed specifically for the DHS Securing-the-Cities initiative and Human Portable Tripwire program, in response to the US Department of Homeland Security (DHS) needs. The BCU runs the same data collection and analysis software developed for the 1"x2" and 2"x2" Detection Devices (DD) and software developed for the SmartShield G300 and G500 Radiation Detectors to support user interface requirements of the Samsung Galaxy s6 smartphones.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Panasonic "TOUGHBOOK 31" Laptop; CPU: Intel® Core™ i5-3380M vPro™ Processor; 2.9GHz with Turbo Boost up to 3.6GHz; Intel Smart Cache 3MB; Intel® Core™ i5-3340M vPro™ Processor; 2.7GHz with Turbo Boost up to 3.4GHz; Intel Smart Cache 3MB; Intel® Core™ i3-3120M Processor; 2.5GHz; Intel Smart Cache 3MB</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>Panasonic "TOUGHBOOK 31" Laptop transmits signals and messages to the Intelligent Radiation Sensor Systems (IRSS) 1"x2" and 2"x2" Detection Devices (DD), and the Network Sensor System (Nets²) SmartShield G300 and G500 Radiation Detectors. (cell phone detection devices).</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>Panasonic "TOUGHBOOK 31" Laptop receives signals and messages from the Intelligent Radiation Sensor Systems (IRSS) 1"x2" and 2"x2" Detection Devices (DD), and the Network Sensor System (Nets²) SmartShield G300 and G500 Radiation Detectors. (cell phone detection devices).</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Optional integrated 4G LTE multi carrier mobile broadband with satellite GPS; Optional GPS (SiRFstarIII™); Intel® Centinno® Advanced-N 6235 802.11a/b/g/n; Bluetooth® v4.0 + EDR (Class 1);</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Wireless: n Optional integrated 4G LTE multi carrier mobile broadband with satellite GPS; Optional GPS (SiRFstarIII™); Intel® Centinno® Advanced-N 6235 802.11a/b/g/n; Bluetooth® v4.0 + EDR (Class 1); Security; Authentication: LEAP, WPA, 802.1x, EAP-TLS, EAP-FAST, PEAP; Encryption: CKIP, TKIP, 128-bit and 64-bit WEP, Hardware AES; User-selectable antenna pass-through (dual standard, single optional); Slide on/off switch</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>Security features: Password Security: Supervisor, User, Hard Disk Lock; Kensington cable lock slot; Trusted platform module (TPM) security chip v.1.22; Computrace theft protection agent in BIOS8; Intel® Anti-Theft Technology; Optional fingerprint reader; Optional insertable SmartCard reader</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Integrated Options: 4G LTE multi carrier mobile broadband with satellite GPS; GPS (SiRFstarIII™); Webcam2; 2nd LAN (10/100)2 or Modem; Insertable SmartCard reader; Fingerprint reader; Media bay 2nd battery¹</p> <p>Security features: Password Security: Supervisor, User, Hard Disk Lock; Kensington cable lock slot; Trusted platform module (TPM) security chip v.1.22; Computrace theft protection agent in BIOS8; Intel® Anti-Theft Technology; Optional fingerprint reader; Optional insertable SmartCard reader</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
---	--	---

<p>Bluetooth® v4.0 + EDR (Class 1)</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Fingerprint reader. Security; Authentication: LEAP, WPA, 802.1x, EAP-TLS, EAP-FAST, PEAP</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>Optional integrated 4G LTE multi carrier mobile broadband with satellite GPS; Intel® Centino® Advanced-N 6235 802.11a/b/g/n; Bluetooth® v4.0 + EDR (Class 1)</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

Oshkosh Defense Autonomous Unmanned Ground Vehicle (UGV) “TerraMax”	Patent #: RE 43,891; Independent Claim 44	Patent #: RE 43,891; Dependent Claims
<p>U.S. defense contractor Oshkosh Defense autonomous unmanned ground vehicle (UGV) “TerraMax” is now equipped with radar and LIDAR, which stands for Light Detection and Ranging, is a remote sensing method that uses light in the form of a pulsed laser to measure ranges; uses lasers to detect nearby objects, along with a drive-by-wire system that electronically controls engine speed, transmission, braking, and steering. The system does more than steer and hit the throttle and brakes. It can intelligently control the driveline locks to navigate deep sand or mud, without input from the operator. The “TerraMax” technology has recently completed its first technical assessment (LTA) for the U.S. Marine Corps UGV (CUGV) initiative. The Cargo UGV program is sponsored by the Marine Corps Warfighting Laboratory and the Joint Ground Robotics Enterprise Robotics Technology Consortium.</p>	<p>A vehicles' stall-to-stop system or vehicle slowdown system in signal communication with a pre-programmed automated system is adapted, modified, or designed to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:</p>	<p>55. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.</p>

<p>“TerraMax”: Drive-by-wire can refer to a number of electronic systems that take the place of old mechanical controls. Instead of using cables, hydraulic pressure, and other things that provide the driver with direct, physical control over the speed or direction of a vehicle, drive-by-wire technology uses electronic controls to activate the brakes, control the steering, and operate other systems.</p>	<p>an electrical system in electrical communication with at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>TerraMax, a leading contributor to autonomous vehicle technology, has computer-controlled steering, acceleration, braking and transmission, a new laser scanner offers enhanced sensing abilities and 360° obstacle detection, as well as the ability to reduce the visual signature of the vehicle's sensors so that it can better blend in with military fleets.</p>	<p>a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>“TerraMax”: Drive-by-wire can refer to a number of electronic systems that take the place of old mechanical controls. Instead of using cables, hydraulic pressure, and other things that provide the driver with direct, physical control over the speed or direction of a vehicle, drive-by-wire technology uses electronic controls to activate the brakes, control the steering, and operate other systems.</p>	<p>a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of, navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot pedal, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>“TerraMax”, a leading contributor to autonomous vehicle technology, has computer-controlled steering, acceleration, braking and transmission, a new laser scanner offers enhanced sensing abilities and 360° obstacle detection, as well as the ability to reduce the visual signature of the vehicle's sensors so that it can better blend in with military fleets.</p>	<p>a receiver in computer communication with the computer system and adapted to receive at least one control signal in response to one of the vehicle's operating systems for monitoring the vehicle's condition upon exceeding a pre-programmed vehicle operating system parameter from the pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means such that the speed of the vehicle is initially decreased immediately after activation of the means upon initial receipt of the at least one control signal; and</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of, navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot pedal, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>“TerraMax”: Drive-by-wire can refer to a number of electronic systems that take the place of old mechanical controls. Instead of using cables, hydraulic pressure, and other things that provide the driver with direct, physical control over the speed or direction of a vehicle, drive-by-wire technology uses electronic controls to activate the brakes, control the steering, and operate other systems. “TerraMax”, a leading contributor to autonomous vehicle technology, has computer-controlled steering, acceleration, braking and transmission, a new laser scanner offers enhanced sensing abilities and 360° obstacle detection, as well as the ability to reduce the visual signature of the vehicle’s sensors so that it can better blend in with military fleets.</p>	<p>wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor.</p>	<p>27. The vehicles’ stall-to-stop means or the vehicles’ slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
--	--	--

Dream Hammer's "Ballista" Software for Computer, Tablet or Smartphone	Patent #: RE 43,891; Independent Claim 44	Patent #: RE 43,891; Dependent Claims
<p>Its first product, Ballista, is an OS for drones and allows one person to simultaneously control multiple drones of any type. It features a plug and play architecture that can be integrated into any unmanned system. Ballista has been licensed to government agencies including the U.S. Navy's Program Executive Office (PEO) Unmanned Aviation and Strike Weapons. Owners of separate systems can share software, which over the long run could save the Defense Department billions of dollars in software costs, officials predict. On July 3, 2013, DreamHammer announced it was partnering with Lockheed Martin to use the company's software for integrated command and control of Lockheed Martin's unmanned aerial vehicles. Lockheed and the Pentagon have worked with DreamHammer to create the software which works with boats, planes or trucks. Ballista open software platform allows for autonomous and simultaneous control. Autonomous and unmanned vehicles involve a transfer of control from direct human input to automated or remote control.</p>	<p>A vehicles' stall-to-stop system or vehicle slowdown system in signal communication with a pre-programmed automated system is adapted, modified, or designed to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:</p>	<p>55. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 44], further can be adapted, modified or designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.</p>

<p>The first step towards an autonomous vehicle is the implementation of a drive-by-wire system: Drive-by-wire can refer to a number of electronic systems that take the place of old mechanical controls. Instead of using cables, hydraulic pressure, and other things that provide the driver with direct, physical control over the speed or direction of a vehicle, drive-by-wire technology uses electronic controls to activate the brakes, control the steering, and operate other systems. Autonomous Emergency Braking (AEB) is a function which use radar or LIDAR sensors; detects upcoming obstacles; takes action to prevent a collision.</p>	<p>an electrical system in electrical communication with at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>DreamHammer's Ballista software has computer-controlled steering, acceleration, braking and transmission; a laser scanner that offers enhanced sensing abilities and obstacle detection. It is designed to military and safety-critical standards, works with all unmanned drones and robots, and can be used to link multiple drones into one master system, all controlled by one person. Ballista is built on an open software platform which allows for autonomous and simultaneous control of multiple unmanned vehicles across all domains-space, air, sea, and land-and can be run from virtually any computer, including a tablet or smartphone.</p>	<p>a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>The first step towards an autonomous vehicle is the implementation of a drive-by-wire system: Drive-by-wire can refer to a number of electronic systems that take the place of old mechanical controls. Instead of using cables, hydraulic pressure, and other things that provide the driver with direct, physical control over the speed or direction of a vehicle, drive-by-wire technology uses electronic controls to activate the brakes, control the steering, and operate other systems. Autonomous Emergency Braking (AEB) is a function which use radar or LIDAR sensors; detects upcoming obstacles; takes action to prevent a collision.</p>	<p>a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of, navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot pedal, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
<p>DreamHammer's Ballista software has computer-controlled steering, acceleration, braking and transmission; a laser scanner that offers enhanced sensing abilities and obstacle detection. It is designed to military and safety-critical standards, works with all unmanned drones and robots, and can be used to link multiple drones into one master system, all controlled by one person. Ballista is built on an open software platform which allows for autonomous and simultaneous control of multiple unmanned vehicles across all domains-space, air, sea, and land-and can be run from virtually any computer, including a tablet or smartphone.</p>	<p>a receiver in computer communication with the computer system and adapted to receive at least one control signal in response to one of the vehicle's operating systems for monitoring the vehicle's condition upon exceeding a pre-programmed vehicle operating system parameter from the pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means such that the speed of the vehicle is initially decreased immediately after activation of the means upon initial receipt of the at least one control signal; and</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of, navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot pedal, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>

<p>The first step towards an autonomous vehicle is the implementation of a drive-by-wire system: Drive-by-wire can refer to a number of electronic systems that take the place of old mechanical controls. Instead of using cables, hydraulic pressure, and other things that provide the driver with direct, physical control over the speed or direction of a vehicle, drive-by-wire technology uses electronic controls to activate the brakes, control the steering, and operate other systems.</p> <p>DreamHammer's Ballista software has computer-controlled steering, acceleration, braking and transmission; a laser scanner that offers enhanced sensing abilities and obstacle detection. It works with all unmanned drones and robots, and can link multiple drones into one master system; controlled by one person. Ballista is built on an open software platform which allows for autonomous and simultaneous control of multiple unmanned vehicles across all domains-space, air, sea, and land-and can be run from virtually any computer, including a tablet or smartphone.</p>	<p>wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot pedal, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor.</p>	<p>27. The vehicles' stall-to-stop means or the vehicles' slowdown means [of claim 23], further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot pedal, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.</p>
---	---	---

“COINS” Nano-Embedded Sensors for Smartphones	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>“COINS” Nano-Embedded Sensors for Smartphones: The Center of Integrated Nanomechanical Systems (COINS) is a multidisciplinary nanoscale science and engineering center (NSEC) funded by the National Science Foundation with its headquarters at the University of California at Berkeley and satellite campuses at Stanford, Caltech, and University of California at Merced.</p> <p>The goal of COINS is to develop and integrate cutting-edge nanotechnologies into a versatile platform with various ultra-sensitive, ultra-selective, self-powering, mobile, wirelessly communicating detection applications; develop novel low-power, low-cost, selective nanomaterials-enable sensing systems for real-time detection of explosives, toxicants, and radiation and interface Nano-enable sensors with smart phones, eventually becoming embedded in the device.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. Apple A4 is based on the ARM processor architecture. The first version released runs at 1 GHz for the iPad and contains an ARM Cortex-A8 CPU core.</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi).</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>The "COINS" Nano-Embedded Sensors for the Apple iPhone and Apple iPad communication devices receives signals from, and transmits signals to any of one or more products listed in any of the plurality of design similarities to include but is not limited to, stall, stop or vehicle slowdown systems; disabling lock systems; biometrics systems; near field communication systems; detection systems, and communication/monitoring devices and systems, through software application downloads, physical interfaces, gateways, processors and communication means and methods (e.g. Bluetooth; long and/or short radio frequency (RF)).</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition... ; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Apple's "Touch ID", a fingerprint identity sensor that makes it easy to get into the iPad device. The biometric "Touch ID" is used with the iPhone 5s or later, iPad Pro, iPad Air 2, or iPad mini 3 or later. Figure 1 image from the 2008 Apple patent 20100082444 showing NFC Logo and fingerprint scanner (e.g., NFC + Fingerprint Scanner). The image displays the NFC Logo at the top and the Fingerprint Sensor at the bottom. The image is from published patent application 20100082444 filed on September 30, 2008 and is now patent [9,026,462] issued May 05, 2015. In this patent Apple speaks a great deal about biometrics and more directly fingerprint scanner built into the face of the illustrated Apple iPhone (#45)</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

Variable's "NODE+Oxa" for the Apple (iPhone) Smartphone	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>Variable's "NODE+Oxa" for the Apple (iPhone) Smartphone. In 2007, when the Department of Homeland Security (DHS) issued a call for a sensor that could equip a smartphone with the ability to detect dangerous gases and chemicals, NASA Ames Research Center scientist Jing Li proposal in response to DHS's Cell-All initiative was awarded funding through an interagency agreement in 2008. Li approached George Yu of Genel Systems Inc. The team settled on the iPhone, which was new at the time, and Li convinced the program manager at DHS that the sensor should be a module attached to the outside of the phone, rather than a system built into the phone's guts. After founding Variable Inc. Yu commercialize the NODE+Oxa which accurately measures the levels of carbon monoxide, nitric oxide, nitrogen dioxide, chlorine gas, sulfur dioxide, or hydrogen sulfide in an indoor environment. It can store data or transmit it to a smartphone using Bluetooth wireless technology.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. Apple A4 is based on the ARM processor architecture. The first version released runs at 1 GHz for the iPad and contains an ARM Cortex-A8 CPU core.</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi).</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Variable's "NODE+Oxa" for the Apple (iPhone) Smartphone communication devices receives signals from, and transmits signals to any of one or more products listed in any of the plurality of products grouped by common features of design similarities to include but is not limited to, stall, stop or vehicle slowdown systems; disabling lock systems; biometrics systems; near field communication systems; detection systems, and</p> <p>communication/monitoring devices and systems, through software application downloads, physical interfaces, gateways, processors and communication means and methods (e.g. Bluetooth; long and/or short radio frequency (RF)).</p>		<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition...; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Apple's "Touch ID"; a fingerprint identity sensor that makes it easy to get into the iPad device. The biometric "Touch ID" is used with the iPhone 5s or later, iPad Pro, iPad Air 2, or iPad mini 3 or later. Figure 1 image from the 2008 Apple patent 20100082444 showing the NFC Logo and fingerprint scanner (e.g., NFC + Fingerprint Scanner). The image displays the NFC Logo at the top and the Fingerprint Sensor at the bottom. The image is from published patent application 20100082444 filed on September 30, 2008 and is now patent [9,026,462] issued May 05, 2015. In this patent Apple speaks a great deal about biometrics and more directly fingerprint scanner built into the face of the illustrated Apple iPhone (#45)</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

Smartphone-Based Rapid Diagnostic Tests	Patent #: 9,096,189; Independent Claim 1	Patent #: RE 43,990; Dependent Claims
<p>The chemical and biomolecular engineering department at the UH Cullen College of Engineering have won the National Science Foundation's Innovation Corps (I-Corps) award. The UH I-Corps team will use the \$50,000 award to develop highly sensitive rapid medical diagnostic tests that use "glow-in-the-dark" nanoparticles to signal the presence of a disease target. Using phosphorescent nanoparticles and a light-based readout allow much more sensitive, quantitative and reliable test results.</p> <p>Moreover, Raja said an inexpensive smartphone attachment, designed like a phone case, could be manufactured that would allow the test results to be read with the phone's built-in camera and flash. "A user would have to add the sample, such as a fingerprick quantity of blood, to a disposable test cartridge containing our nanoparticles, and then insert it into the smartphone attachment after 15 minutes. The flash from the camera will excite the luminescent particles, and the smartphone camera will capture the light emitted by them," Raja said.</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>18. The communication device [of claim 11] wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring.</p>

<p>Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. Apple A4 is based on the ARM processor architecture. The first version released runs at 1 GHz for the iPad and contains an ARM Cortex-A8 CPU core.</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;</p>	<p>12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi).</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween;</p>	<p>20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.</p>
<p>If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.</p>

<p>Smartphone-Based Rapid Diagnostic Tests communication devices receives signals from, and transmits signals to any of one or more products listed in any of the plurality of products grouped by common features of design similarities to include but is not limited to, stall, stop or vehicle slowdown systems; disabling lock systems; biometrics systems; near field communication systems; detection systems, and communication/monitoring devices and systems, through software application downloads, physical interfaces, gateways, processors and communication means and methods (e.g. Bluetooth; long and/or short radio frequency (RF)).</p>		<p>32. The communication device [of claim 11] wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition... ; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>

<p>Apple's "Touch ID", a fingerprint identity sensor that makes it easy to get into the iPad device. The biometric "Touch ID" is used with the iPhone 5s or later, iPad Pro, iPad Air 2, or iPad mini 3 or later. Figure 1 image from the 2008 Apple patent 20100082444 showing NFC Logo and fingerprint scanner (e.g., NFC + Fingerprint Scanner). The image displays the NFC Logo at the top and the Fingerprint Sensor at the bottom. The image is from published patent application 20100082444 filed on September 30, 2008 and is now patent [9,026,462] issued May 05, 2015. In this patent Apple speaks a great deal about biometrics and more directly fingerprint scanner built into the face of the illustrated Apple iPhone (#45)</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.</p>
<p>Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).</p>	<p>25. The communication device of [claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.</p>